Centers for Medicare & Medicaid Services (CMS)
Business Partners
Systems Security Manual

CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES
SYSTEMS SECURITY GROUP
7500 SECURITY BOULEVARD
BALTIMORE, MD 21244-1850

(Rev. 8, 04-06-07)

CMS/Business Partners
Systems Security Manual
Table of Contents
(Rev. 8, 04-06-07)

Transmittals Issued for this Manual

Appendices

Record of Changes

(Rev. 8, 04-06-07)

Revision	***Major Changes***	***Date***
3.0	*Removed Appendix B, Triennial Risk Assessment Guide, re-lettered all appendices accordingly, and updated all references to the appendices within the document accordingly.* *Re-wrote Appendix B (formerly Appendix C), Medicare Information Technology (IT) Systems Contingency Planning.* *Re-wrote sections 3.1, 3.2, and 3.3* *Included correct links to the CMS website.* *Changed some verbiage in Table 3.1.* *Included a Record of Changes page.*	*12/20/02*
3.1	*Added a second link to HIPAA in section 1.* *Added Risk Assessment Methodology to section 1.* *Added text to Table 3.1.*	*3/31/03*
3.2	*Changed the URL for GAO/AMID-12.19.6 (FISCAM) reference in section 1.* *Added definitions for types of testing in Appendix B, section 6.* *Updated the Appendix E, Glossary.*	*8/31/03*
3.3	*Changed entry in Comments of Item 3.3 in Table 3.1.*	*8/31/03*

Revision	Major Changes	Date
	Changed last paragraph in section 3.3.	
3.4	*Re-wrote entire section 4.2, Sensitive Information Protection Requirements.* *Updated section 5.0, Internet Security, requirement documents.* *Re-wrote entire Appendix A, section 2.0, The Contractor Assessment Security Tool (CAST).* *Revised the Appendix A, section 2.0, "Status" Decision Tree.* *Updated the Appendix E, Glossary.* *Made minor editorial changes throughout document.*	*11/30/03*
4.1	*Re-wrote section 5.0, Internet Security to integrate CMS CRs 1439 and 1749 relating to Internet Policy.*	*02/27/04*
4.2	*Inserted section 3.9, Patch Management.* *Revised section 3.5.1, Annual Compliance Audit (ACA).* *Added a reference to section 1.0.* *Made some editorial changes.*	*05/31/04*
4.3	*Changed CSRs to incorporate Acceptable Risk Safeguards (ARSs), PSC and COB guidance, and clarification of Self-Assessment response instructions.* *Added section 3.10, Security Management Resources.* *Modified section 3.9, Patch Management.* *Modified section 3.5.2, Corrective Action Plans and Plans of Action and Milestones.* *Made some editorial changes.*	*09/30/04*
4.4	*Added language throughout section 3 to clarify deliverable formats, media, and schedules, and to add language about various Acts and directives that have security assessment implications for CMS.* *Renamed and modified section 3.5.2, Corrective Action Management Process and Plans of Action and Milestones.* *Changed all instances of "Corrective Action Plan" and/or "CAP" to "Corrective Action Management Process."* *Modified section 5.0, Internet Security.* *Rewrote Appendix A to correspond with recent Tool Suite enhancements.* *Added some document references, updated some hyperlinks, and made other editorial changes.*	*11/19/04*
6.1	*Inserted a new Appendix D, CMS Information Security Guidebook for Audits; shifted appendix numbers for sections previously marked Appendix D and E (now E and F, respectively).* *Reorganized lists of references to group like citations together.* *Updated the list of STIGs (table 3.2 in section 3.10.1) to reflect most current documents, ensure working links, and add missing document references.* *Added MAC language (sections 1.0 and 1.1).* *Updated Reporting Requirements (section 3.0) per recent CMS*	*02/06*

Revision	Major Changes	Date
	Memorandum and completely re-wrote, and re-titled, section 3.5.2. *Added/modified definitions for glossary terms that pertain to reporting requirements.* *Revised the Appendix A "Status" Decision Tree.* *Added a text reference and citation for the CMS Policy for the Information Security Program.* *Revised, restructured Appendix A to replace CAST procedures that no longer apply with CISS tool business rules and form use instructions; added guidance for creating findings, weaknesses, and action plans.* *Modified Appendix A response status information to align with CISS business rules.* *Various other editorial changes.*	
8.0	*Main Document and all appendices: Stylized the Main document and all Appendices to be identical.* *1.0: Updated CMS contract types and list of document references.* *1.1: Grammar and style corrections.* *2.2: Grammar and style corrections.* *2.3: Grammar and style corrections. Vocabulary clarifications.* *3.0: Grammar and style corrections. Modified Table 3.1 to update security reporting requirements. Updated Table 3.1 legend. Updated the CMS contact information.* *3.1: Grammar and style corrections. Updated wording for clarity. Updated CISS help desk phone number.* *3.2: Grammar and style corrections. Updated wording for clarity.* *3.3: Updated ACA requirements. Updated CISS help desk phone number. Updated wording for clarity.* *3.4 through 3.5.2.2: Grammar and style corrections. Updated wording for clarity. Updated CISS help desk phone number.* *3.5.3: Added Section 3.5.3, Annual/Yearly Compliance Condition.*	*12/2006*

Revision	Major Changes	Date
	3.6 and 3.61: Removed the CMS Service Desk contact requirement. Updated Security Incident response requirements. Grammar and style corrections. Updated wording for clarity. *3.7: Updated ACA requirements. Grammar and style corrections. Updated wording for clarity.* *3.8 and 3.9: Grammar and style corrections. Updated wording for clarity.* *3.10.1: Removed and updated STIG contents into new Appendix F.* *3.10.2: Updated the list of NIST SP and FIPS to reflect the most current documents.* *4.0 through 4.1.3: Rewrote section 4.1, Security Impact Levels, and all of its subsections to incorporate FIPS Pub 199 security categorization standards and the CMS "HIGH" security level designation. Revised table 4.1 to summarize the FIPS Pub 199 security impact levels. Added table 4.2 to summarize the FIPS Pub 199 security objective potential impact definitions.* *4.2: Revised section to incorporate the CMS "HIGH" security level designation.* *Appendix A: Revised Appendix A Section 2.8.2.9, Determining Risk, and its subsections to update the likelihood of occurrence, impact severity, and level of risk determination criteria and tables. Grammar and style corrections. Updated wording for clarity.* *All Appendices: Inserted new Appendices E and F. Existing Appendices renumbered. Grammar and style corrections. Updated wording for clarity.*	

1.0 - Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information technology (IT) systems security controls in order to maintain the confidentiality, integrity, and availability of Medicare systems operations in the event of computer incidents or physical disasters.

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, Fiscal Intermediaries, Common Working File (CWF) host sites, standard claims processing system maintainers, regional laboratory carriers, claims processing data centers, *Data Centers, Enterprise Data Centers (EDCs), and* Medicare Administrative Contractors (MACs) *(including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC])*.

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 - SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). In this manual the terms "business partner" and "contractor" are used interchangeably, and all provisions that apply to business partners also apply to MAC contractors.

This manual addresses the following key business partner security elements:

- An overview of primary roles and responsibilities
- A program management planning table that will assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites
- Appendix A: The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs), which provides the following:
    - *The CSRs*
    - *An overview of the CISS data collection and reporting process*

The CMS IT systems security program and CSRs were developed in accordance with Federal and CMS documents that mandate the handling and processing of Medicare data. These documents include the following:

- CMS System Security Plans (SSP) Methodology, Version 3.0, *October 28*, 2002 *http://www.cms.hhs.gov/InformationSecurity/Downloads/ssp_meth.pdf*
- Federal Information Security Management Act of 2002 (FISMA), November 27, 2002 http://csrc.nist.gov/policies/FISMA-final.pdf
- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996 http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm
- GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999

http://www.gao.gov/special.pubs/ai12.19.6.pdf

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, June 2000
  http://www.irs.gov/pub/irs-pdf/p1075.pdf

- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (PUBLIC LAW 108–173), DEC. 8, 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors
  http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf

- Office of Management and Budget (OMB) Circular No. A-127, Financial Management Systems, June 21, 1995
  http://www.whitehouse.gov/omb/circulars/a127/a127.html

- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999
  http://www.whitehouse.gov/omb/circulars/index.html

- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000
  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000
  http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

- Presidential Decision Directive/NSC – 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998
  http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

- Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to provider of service
  http://www.ssa.gov/OP_Home/ssact/title18/1816.htm

- Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits
  http://www.ssa.gov/OP_Home/ssact/title18/1842.htm

- Public Law 93-579, The Privacy Act of 1974, as amended
  http://www.usdoj.gov/foia/privstat.htm

- Public Law 99-474, Computer Fraud & Abuse Act of 1986
  http://nsi.org/Library/Compsec/cfa.txt

- Public Law 100-235, Computer Security Act of 1987

http://www.nist.gov/cfo/legislation/Public Law 100-235.pdf

- Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35
  http://www.estrategy.gov/documents/16.pdf

- Public Law 104-106, Clinger-Cohen Act of 1996 (formerly called the Information Technology Management Reform Act)
  http://www.tricare.osd.mil/jmis/download/PublicLaw104_106ClingerCohenActof1996.pdf

- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA), 1996
  http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAlawdetail.pdf

- Public Law 106-398, National Defense Authorization Fiscal Year 2001, Government Information Security Reform Act (GISRA) of 2000
  http://peoammo.army.mil/PEOAMMO/CIO Web/CIO References/US Code Extracts/PL 106-398 Sec 811.doc

Additional documents were used as references in the development of this manual and the CMS CSRs. These documents include the following:

- CMS Information Security Acceptable Risk Safeguards (ARS) Version *2.0*, *March 13,2006*
  http://www.cms.hhs.gov/InformationSecurity/Downloads/ars.pdf

- CMS Information Security Certification and Accreditation (C&A) Methodology, Version 1.0, May 12, 2005
  http://www.cms.hhs.gov/InformationSecurity/Downloads/C&A_meth.pdf

- CMS Information Security Risk Assessment (RA) Methodology, Version 2.1 April 22, 2005
  http://www.cms.hhs.gov/InformationSecurity/Downloads/RA_meth.pdf

- CMS Information Security Risk Assessment (RA) and System Security Plan (SSP)Guidance, Version # 1.0 September 3, 2004
  http://www.cms.hhs.gov/InformationSecurity/Downloads/ra_and_ssp_guidance.pdf

- Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731
  http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html

- United States Code Title 44 Chapter 33—Disposal of Records
  http://www4.law.cornell.edu/uscode/html/uscode44/usc_sup_01_44_10_33.html

- Department of Health and Human Services (DHHS), IRM Policies and Guidelines
  http://www.hhs.gov/read/irmpolicy/index.html

- Homeland Security Presidential Directive/HSPD-7
  http://www.fas.org/irp/offdocs/nspd/hspd-7.html

- National Institute of Standards and Technology SP 800-26, Security Self Assessment Guide for Information Technology Systems, November 2001
  http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, SP800-12
  http://csrc.nist.gov/publications/nistpubs/800-12

- NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide, January 2004
  http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004
  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html.

- CMS Policy for the Information Security Program, *CMS-CIO-POL-SEC02,* May 2005
  http://www.cms.hhs.gov/InformationSecurity/Downloads/policy_is_program.pdf

1.1 - Additional Requirements for MAC Contractors

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

MAC contractors are responsible for fulfilling all existing business partner requirements. *A*dditional requirements are specified in Section 912 of the Medicare Modernization Act (MMA). These additional requirements include the following:

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.

- The contractor shall comply with the CMS Certification and Accreditation (C&A) methodology, policies, standards, procedures, and guidelines for contractor facilities and systems. The CMS C&A methodology can be found on the CMS web site *at: http://www.cms.hhs.gov/InformationSecurity/Downloads/C&A_meth.pdf*.

- The contractor shall conduct or undergo an independent evaluation and test of its system security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under the contract.

- The contractor shall support CMS validation and accreditation of contractor systems and facilities in accordance with *the* CMS C&A methodology.

- The contractor shall provide annual certification, in accordance with *the CMS* C&A methodology, that they have examined the management, operational, and technical controls for its systems supporting the MAC function, and consider these controls adequate to meet CMS security standards and requirements.

The contractor shall appoint a Chief Information Officer *(CIO)* to oversee its compliance with the CMS security requirements. The contractor's *Systems Security Officer (*SSO*)* shall be a full-time position dedicated to assisting the CIO in fulfilling the*se* requirements.

2.0 - IT Systems Security Roles and Responsibilities

(Rev. 3, 03-28-03)

2.1 - Consortium Contractor Management Officer and CMS Project Officer (CCMO/PO)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The Consortium consists of four offices (Northeastern, Southern, Midwestern, and Western). The CCMO is a part of the Consortium and is responsible for CMS contract management activities. CCMOs are responsible for the oversight of Medicare carriers and fiscal intermediaries. CMS POs (generally located in Central Office business components) oversee the other business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The CCMO/PO has the following responsibilities:

- CMS point of contact for business partner IT systems security problems
- Central point for the reception of IT SSPs and reports including security incident reports
- Provider of technical assistance necessary to respond to CMS security policies and procedures.

2.2 - The (Principal) Systems Security Officer (SSO)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partners must designate an SSO qualified to manage the Medicare system security program and ensure the implementation of necessary safeguards. The SSO must be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development.

The SSO position for each contractor should be full-time and fully qualified—preferably credentialed in systems security *(e.g., Certified Information Systems Security Professional [CISSP]).* Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. *A* qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization.

A sound entity-wide security program is the cornerstone of effective security control implementation and maintenance. *Security* controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available Line One funding.

A business partner may have additional SSOs at various organizational levels, but *all* security actions *must be coordinated* through the principal SSO for Medicare records and operations. The SSO ensures compliance with CMS CSRs by:

- Facilitating the Medicare IT system security program and ensuring that necessary safeguards are in place and working
- Coordinating system security activities throughout the organization
- Ensuring that IT system security requirements are considered during budget development and execution
- Reviewing compliance of all components with the CMS CSRs and reporting vulnerabilities to management
- Establishing an incident response capability, investigating system security breaches, and reporting significant problems (see section 3.6) to business partner management and *the CCMO.*
- Ensuring that technical and operational security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes
- Ensuring that IT systems security requirements are included in *Requests for Proposal (*RFP*)* and subcontracts involving the handling, processing, and analysis of Medicare data
- Maintaining systems security documentation in the System Security Profile for review by CMS and external auditors
- Cooperating in all official external evaluations of the business partner's system security program
- Facilitating the completion of the Risk Assessment (see section 3.2)
- Ensuring that an operational IT Systems Contingency Plan is in place and tested (see section 3.4)
- Documenting and updating the monthly Plan of Action and Milestones (POA&M*) (*see section 3.5.2). Updates may occur whenever a POA&M projected completion date

passes, and following the issuance of new requirements, risk assessments, internal audits, and external evaluations. The schedule and updates are highly sensitive and should have limited distribution.

- Keeping all elements of the business partner's System Security Profile secure (see section 3.7)

- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix B)

The Principal SSO should earn *a minimum of* 40 hours *in* continuing professional education credits each year from a recognized national information systems security organization. The educational sessions at the *CMS S*ecurity *B*est *P*ractices *C*onference can be used toward fulfilling CMS business partners' continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the *CMS S*ecurity *B*est *P*ractices *C*onference agenda.

2.3 - System Owners/Managers

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partner System Owners/Managers are responsible for:

- Determining and documenting the *information and information system security levels* of the resources for which they are responsible

Identifying appropriate security level *categorizations* for their *information* systems

2.4 - System Maintainers/Developers (Rev. 3, 03-28-03)

Business partner System Maintainers/Developers have the responsibility to implement the security requirements throughout the System Development Life Cycle (SDLC) using the security level designation as the basis.

2.5 - Personnel Security/Suitability

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

All business partner and contractor employees requiring access to CMS sensitive information must meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum: contacting references provided by the employee and contacting the local law enforcement agency or agencies.

3.0 - IT Systems Security Program Management

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partners must have policies and procedures, and implement controls or plans that fulfill the CMS CSRs (see Attachment A).

Policies are formal, up-to-date, documented rules stated as "shall" or "will" statements that exist and are readily available to employees. They establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up-to-date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Controls are measures implemented to protect the confidentiality, integrity, and availability of sensitive information. IT security procedures and controls shall be implemented in a consistent manner everywhere that the procedure applies. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that controls are operating as intended.

*M*eeting requirements does not validate the quality of a program. Managers with oversight responsibility must understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and provides high-level descriptions for them. As appropriate, *Table 3.1* refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners must perform a Self-Assessment using the *CISS*. The weaknesses, action plans, and POA&Ms must be recorded in the CISS (*S*ee Appendix A). To perform the Self-Assessment, business partners must conduct a systematic review of the CSRs using the CISS. The CISS provides a Self-Assessment form that includes guidance and audit protocols to assist in the review of the requirements.

The CMS CSRs include key security-related tasks. Table 3.1 indicates how often these tasks need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a “do by” date. The number accompanying each entry in the requirement column indicates the section in this document that deals with the particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Table 3.1. Reporting Requirements Planning Table

Requirement	Frequency	Send To	Comments	Complete (check when complete)
Appendix A, Self-Assessment using the CISS	Each Federal FY	▪ CCMO/PO with a copy to CMS CO ▪ System Security Profile	See Appendix A for an overview of the CISS. Self-Assessment results recorded using the CISS are to be discussed in the Certification Package.	
3.1 System Security Plans	The SSP for each GSS & MA must be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change[1].	▪ SSO ▪ CMS CO ▪ *System Security Profile*	SSPs are to be reviewed, updated, and certified by management and indicated as such in both the Certification Package/statement of certification and the System Security Profile[2].	
3.2 Risk Assessment (Report)	The Risk Assessment for each GSS and MA must be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change.[1]	▪ CMS CO ▪ *System Security Profile*	Risk Assessments are to be reviewed, updated, and certified by management and indicated as such in both the Certification Package/statement of certification and the System Security Profile. The Risk Assessment Report *submitted with* the *SSP*[3].	
3.3 Certification	Each Federal FY	▪ CCMO/PO with a copy to CMS CO ▪ System Security Profile	Fiscal intermediaries and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-6) information on certification requirements including where, when, and to whom these certifications must be submitted. All other contractors should submit a statement of security certification to their CMS POs.	
3.4 **IT Systems Contingency Plan**	Contingency Plans must be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change.[1] Plans must be tested annually.	▪ SSO ▪ CMS CO ▪ *System Security Profile*	Management and the SSO must approve the Plan. The IT *Systems* Contingency Plan is to be developed (in accordance with Appendix B), reviewed, updated, and certified by management—and indicated as such in both the Certification Package/statement of certification and the System Security Profile[4].	

---

[1] NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."

[2] More information about system security planning can be found in the CMS SSP Methodology.

[3] More information about Risk Assessment Reports can be found in the CMS Information Security Risk Assessment (RA) Methodology.

[4] More information about contingency planning can be found in An Introduction to Computer Security: The NIST Handbook. SP 800-12, and the Contingency Planning Guide for Information Technology Systems: NIST Special Pub 800-34.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.5 Compliance	Each Federal FY	▪ *S*SO ▪ *C*CMO/PO ▪ *C*MS CO ▪ *System Security Profile*	POA&Ms address findings of annual system security assessments including the annual CMS Self Assessment Review, and, as applicable: SAS 70 audits, CFO controls audits, the Section 912 evaluation, and data center tests and reviews.	
3.6 Incident Reporting and Response	As necessary	▪ CCMO/PO ▪ System Security Profile	HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file with the *Principal SSO*		

LEGEND:

CCMO	Consortium Contractor Management Officer
CFO	Chief Financial Officer
CISS	CMS Integrated Security Suite
CO	Central Office (CMS)
CPIC	Certification Package for Internal Controls
FY	Fiscal Year
GSS	General Support System
HIPAA	*Health Insurance Portability and Accountability Act*
IT	*Information Technology*
MA	Major Application
PO	Project Officer (CMS)
POA&M	*Plan of Action and Milestones*
SAS	*Statement on Auditing Standard*
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer
SSP	*System Security Plan*

NOTE: Documents listed in table 3.1 may be stored as paper documents, electronic documents, or a combination thereof.

When submitting documentation to CCMOs or to the CMS Central Office, *registered* mail or *its* equivalent (*signed* receipt required) *should be used*. For supporting documentation (such as Risk Assessments, Contingency Plans, System Security Plans, etc.), only digital soft copies in the approved CMS format are required. Paper copies are only required for certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:

Program Safeguard Contractors

- CMS Central Office
  Office of Financial Management
  Program Integrity Group
  Mail Stop *C3-02-16*
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Common Working File & Shared System Maintainers

- *CMS Central Office*

Office of Information Services
Business Application and Management Group
Mail Stop N3-13-27
7500 Security Blvd.
Baltimore, MD 21244-1850

Fiscal Intermediaries /Carriers/ Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC])

- *CMS Central Office*
  Centers for Medicare Management
  Medicare Contractor Management Group
  Mail Stop S1-14-17
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Data Centers & Enterprise Data Centers (EDCs)

- *CMS Central Office*
  Office of Information Services
  Enterprise Data Center Group
  Mail Stop N1-19-18
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Following are the contacts and addresses for the four Consortia:

- Northeast Consortium
  Consortium Contractor Management Officer
  Philadelphia Regional Office, Suite 216
  The Public Ledger Building
  150 S. Independence Mall West
  Philadelphia, PA 19106
  215-861-4191

- Southern Consortium
  Consortium Contractor Management Officer
  Atlanta Regional Office
  Atlanta Federal Center, 4th Floor
  61 Forsyth Street, SW, Suite 4T20
  Atlanta, GA 30303-8909
  214-767-6289

- Midwest Consortium
  Consortium Contractor Management Officer
  Chicago Regional Office
  233 N. Michigan Avenue, Suite 600
  Chicago IL 60601

312-353-9840

- Western Consortium
  Consortium Contractor Management Officer
  San Francisco Regional Office
  75 Hawthorne St. 4th and 5th Floors
  San Francisco, CA 94105-3901
  415-744-3628

3.1 - System Security Plan (SSP)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The objective of an information security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process or store Medicare-related data have some level of sensitivity and require protection. The protection of a system must be documented in an SSP. The completion of an SSP is a requirement of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either a Major Application (MA) or General Support System (GSS) must be covered by SSPs.

The purpose of an SSP is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager (i.e., SSO).

All business partners are required to maintain current SSPs for their Medicare claims-related GSSs and MAs in their *S*ystem *S*ecurity *P*rofiles. The SSP documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the SSP serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The SSP is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, these security plans should be distributed only on a need-to-know basis.

The SSPs must be available to the SSO and business partner certifying official (normally the VP for Medicare Operations), and authorized external auditors as required. The SSO and System Owner/Manager are responsible for reviewing the SSP on an annual basis to ensure that it is up-to-date. The objective of these annual reviews is to verify that the controls selected or installed remain adequate to provide a level of protection to reach an acceptable level of risk to operate the system.

All business partner Medicare claims-related SSPs must be developed in accordance with the most current version of the CMS System Security Plans (SSP) Methodology and the CMS

Information Security RA and SSP Guidance, both of which are available on the CMS Web site at: http://www.cms.hhs.gov/it/security/default.asp. Business partners must also use the most current version of the Microsoft® Word© SSP template, available at the same Web site.

SSPs must be re-certified within 365 days from the last date certified. The SSP must also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update to the SSP needs to occur. The SSP must be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review *and the* updated SSP*, if applicable,* must be placed in the Medicare contractor's System Security Profile*,* and a copy must be provided to the CMS Central Office.

Contractors *updating* their current SSP(s) *or developing new SSP(s) must* include *Medicare claims processing* front-end, back-end, and/or other claims processing *related* systems *using* the most current version of the CMS System Security Plan Methodology. The CMS methodology and template can be found on the CMS website at*:* http://www.cms.hhs.gov/it/security/References/ps.asp. Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions. Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc). These back-end systems include, but are not limited to: print mail, 1099, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

A newly developed or updated SSP must be sent *in electronic form* to the CMS Central Office *on CD-ROM*. *This CD-ROM* must be received by CMS ten (10) working days after the *SSP(s) has* been developed, updated, or re-certified*. T*he original signed, dated CMS SSP certification form (Tab A, Appendix A of the CMS SSP Template) must be submitted in hard copy along with the electronic *CD-ROM* copy. *T*his information should not be submitted to the CMS Central Office via email*—r*egistered mail or its equivalent *(signed receipt required)* should be used.

In summary, the SSP must be updated and re-certified annually unless there are changes as discussed above that would necessitate a more frequent update. Should SSP technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-*272-5725*.

3.2 - Risk Assessment

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partners are required to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology and the CMS Information Security RA and SSP

Guidance. These documents are available at:
http://www.cms.hhs.gov/InformationSecurity/14_standards.asp#TopOfPage.

The CMS Information Security RA Methodology presents a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The methodology describes the steps required to produce an Information Security RA Report for systems *and applications* that require an SSP. This methodology and its resultant report replace the former Triennial RA requirement and report.

All system and information owners must develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach shall be used to determine adequate security and shall include a consideration of the major factors in management such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. The CMS Information Security RA Methodology will be used to prepare an annual Information Security RA Report.

All RAs must be re-certified within 365 days from the last date certified. Medicare contractors must review their RA(s) prior to re-certification to determine if an update is needed. An RA must be performed if a significant change to any information system has occurred. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review and/or the updated RA must be placed in the Medicare contractor's System Security Profile. The updated RA(s) must also be mailed to the CMS Central Office. The RA used to support a SSP(s) cannot be dated more than 12 months earlier than the SSP certification date.

Contractors that must update their current RA(s) must use the most current version of the CMS Information Security RA Methodology. The CMS methodology and template can be found on the CMS website at*: http://www.cms.hhs.gov/it/security/References/ps.asp*.

A newly developed or updated RA that *is submitted with* the SSP must be sent to the CMS Central Office *on CD-ROM*. *This CD-ROM* must be received by CMS ten (10) working days after they have been developed *or* updated. *T*his information should not be submitted to the CMS Central Office via email*—r*egistered mail or its equivalent *(signed receipt required)* should be used.

In summary, the RA must be updated annually unless there are changes to either as discussed above that would necessitate a more frequent update. Should RA technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-*272*-*5725*.

Business partners should refer to the CMS Information Security Acceptable Risk Safeguards (ARS) document to aid in the preparation of a risk assessment. This document can be found at*: http://www.cms.hhs.gov/InformationSecurity/14_standards.asp#TopOfPage*.

3.3 - Certification

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All Medicare business partners are required to certify their system security compliance. Certification is the formal process by which a contract official verifies, initially and then by annual reassessment, that a system's security features meet CMS CSRs. Business partners must self-certify that their organization(s) successfully completed a security Self-Assessment of their Medicare IT systems and associated software in accordance with the terms of their Medicare Agreement/Contract.

Each contractor is required to self-certify to CMS its IT systems security compliance within each Federal fiscal year. This security certification will be included in the Certification Package for Internal Controls (CPIC) or, for contracts not required to submit CPIC certifications, send the security certification to their appropriate CMS POs. CMS will continue to require annual, formal re-certification within each fiscal year no later than September 30, including validation at all levels of security as described in this manual.

Systems security certification must be fully documented and maintained in official records. The *security certification* validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification
- Self-Assessment (see Appendix A)
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.4 and Appendix B)
- Results of the ACA (see section 3.5.1) *(no longer required as of October 1, 2006)*
- Plan of Action and Milestones (see section 3.5.2)

3.4 - Information Technology (IT) Systems Contingency Plan

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All business partners are required to develop and document an IT Systems Contingency Plan that describes the arrangements that have been made and the steps that will be taken to continue IT and system operations in the event of a natural or human-caused disaster. Medicare IT Systems Contingency Plans must be included in management planning and must be:

- Reviewed whenever new systems are planned or new safeguards contemplated
- Reviewed annually to ensure that they remain feasible

- Tested annually. If backup facility testing is done in segments, test each individual Medicare segment every year

Appendix B to this manual provides information on Medicare IT Systems Contingency Plans *and testing methods*. See Item 3.4 in Table 3.1, section 3.0, for other references.

Each Medicare contractor must review its IT Systems Contingency Plan 365 days from the date it was last reviewed or updated to determine if changes to the contingency plan are needed. A contingency plan should be updated if a significant change has occurred. The system contingency plan must also be tested 365 days from the last test performed. Updated plans and test reports (results) should be placed in the contractor's System Security Profile. Business partner management and the SSO must approve newly developed or updated IT Systems Contingency Plans. Information on Medicare IT systems contingency planning can be found in Appendix B.

A newly developed or updated Medicare IT System Contingency Plan must be submitted to CMS within 10 (ten) working days after the business partner's management and SSO have approved it. A copy of the IT System Contingency Plan must be submitted via CD-ROM to the CMS Central Office along with a hard copy of the statement of certification. *T*his information should not be submitted via email. Registered mail or its equivalent should be used.

3.5 - Compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Compliance refers to the contractual obligations of business partners to CMS. *The* components to electronic data processing (EDP) security reporting compliance *are* described in detail in the following subsections.

3.5.1 - Annual Compliance Audit (ACA)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

As of October 1, 2006, Annual Compliance Audits are no longer required.

3.5.2 - Plan of Action and Milestones (POA&Ms)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partners are required to submit a monthly POA&M package which is due by the 1st of each month. The POA&M package consists of a CISS-generated *POA&M* data file and*, if required by CMS, any additional supporting* documentation.

3.5.2.1 - Background

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Federal Information Security Management Act of 2002 (FISMA) requires that Federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency. Additionally, periodic POA&Ms reporting the status of known security

weaknesses for all Federal agency systems must also be submitted to the Office of Management and Budget (OMB). This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under The Federal Managers' Financial Integrity Act of 1982 *[FMFIA]*). In the case of FISMA, any security weakness identified for covered systems must be reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of *business partner security programs* to ensure that they meet the information security requirements imposed by FISMA. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The CISS enables contractors to satisfy reporting requirements for EDP *security-related* findings. *Security-related finding* (and approved action plan) data is entered into the *CISS* following all audits/reviews, from which *the* CISS generates a single monthly submission data file that summarizes the *current* state of security for the business partner. This data file is submitted to CMS as part of the monthly POA&M package.

3.5.2.2 - POA&M Package Components/Submission Format

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

In addition to the initial POA&M reporting that follows each audit/review, summary POA&Ms shall be submitted on the *1st* of each month via the CISS. The CISS shall be populated with EDP *security-related* findings from the Chief Financial Officer's Electronic Data Processing (CFO EDP) Audit, the Section 912 evaluation, data center security tests and evaluations, the SAS 70 review, the Certification Package of Internal Controls (CPIC), and any other EDP *security-related* findings that result from an audit or review, whether internal or external. Corrective actions are to be established in the CISS to address all resulting weaknesses entered therein, and those corrective actions will be reflected in the CISS POA&M (both in the data file and reports).

To ensure consistency, all Medicare contractors must enter into the CISS the Section 912 evaluation, Data Center *Security Test and Evaluation (ST&E)*, and/or CFO EDP Audit POA&Ms that have already been accepted and approved by *CMS* for its EDP findings, as the standard for all future submitted POA&Ms. Findings from other audits, reviews and evaluations (e.g., SAS 70, CPIC, internal audits, etc.) that address the same *security finding* problem should use the same solution (action plan) if it will adequately resolve the identified weakness.

Initial Report. Within 45 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial, manually generated, CMS POA&M Weakness Tracking Form is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation. Upon acceptance from CMS, this information will be entered into the CISS by the Medicare contractor for monthly tracking purposes.

NOTE: Medicare contractors are encouraged to use the draft reports (when available) to prepare their corrective actions for identified findings.

Monthly POA&M Package. On a monthly basis, business partners shall provide updates on progress towards completion of remediation efforts for weaknesses identified from all known sources. *T*he monthly POA&M package *shall* include *a* CD*-ROM that* contain*s* the CISS-generated data file *at its root level* (refer to the POA&M submission instructions in the CISS User Guide). *The naming convention for this file is XXX_POAM(XX-01-200X).mdb where XXX is the acronym for the contractor, and the date is the due date of the report.*

Medicare contractors must submit the monthly POA&M package to the CMS Central Office and their CCMO (for Title XVIII and MAC contracts) or PO (for FAR contracts). *T*his information should not be submitted via email. Registered mail or its equivalent should be used. A copy must also be placed in the System Security Profile.

3.5.3 - Annual/Yearly Compliance Condition

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Many security documents, such as Risk Assessments, SSPs, Contingency Plans, as well as many CMS CSR control techniques (see Appendix A) require annual or yearly performance (e.g., test, submission, recertification, review, update). When such a requirement is to be performed annually or yearly, it is to be performed no later than the one year anniversary date of its previous performance (i.e., within 365 days [366 days in leap years]). The only exceptions to this annual/yearly compliance condition are deliverables whose annual due date are set and distributed by CMS, such as the annual CAST Self-Assessment submission.

If the Business Partner wishes to change the timing cycle of an annual or yearly requirement compliance date, the Business Partner must shorten the timing cycle and not lengthen the annual/yearly timing cycle to attain the new performance date. For example, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the Business Partner desired to change the review date to 5/31/07, they would be required to review the SSP no later than 7/31/06 and again no later than 5/31/07, and no later than 5/31/xx thereafter. However, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the Business Partner desired to change the review date to 9/30/06, they would be required to review the SSP no later than 7/31/06 and again no later than 9/30/06. The next review cycle would then be no later than 9/30/07 and 9/30/XX thereafter.

3.6 - Incident Reporting and Response

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

An incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The business partner must use its security policy and procedures to determine whether the security incident is reportable (as defined below). Upon receiving notification of an IT systems security incident or a suspected incident, the SSO will immediately perform an analysis to determine if an

incident actually occurred. The incident could result in adversely impacting the processing of Medicare data or the privacy of Medicare data. Reportable incidents include:

- **Unauthorized Disclosure:** information disclosure with risk to privacy information or public relations impact
- **Denial of Service:** an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- **Malicious Code:** a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- **Unauthorized Access:** a breach in which person gains logical or physical access to network, system application, data or other resource without permission
- **Inappropriate Usage:** a violation of acceptable computing use policies
- **Multiple Components:** a single incident that encompasses two or more incidents

3.6.1 - Computer Security Incident Response

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All confirmed incidents are considered major risks and must be reported immediately to the CCMO/PO. *Additionally, incidents that involve the loss and or disclosure of personally identifiable information must be reported within 1 hour to the CCMO/PO.* The CCMO/PO should be kept informed of the status of the incident follow-up until the incident is resolved. CCMO/POs should be provided with a point of contact at the Medicare contractor's site for the security incident. The phone numbers for the *applicable* CCMO can be found in the contact address list in section 3. *The CCMO/PO will inform the appropriate CMS Central Office point-of-contact of security incidents.*

When reporting confirmed security incidents, business partners should report the date and time when events occurred or were discovered; names of systems, programs, or networks effected by the incident; and impact analysis. Release of information during incident handling must be on an as-needed *and* need-to-know basis. When other entities should be notified of incidents at external business partner sites, CMS will coordinate with legal and public affairs contacts at the effected entities. If a violation of the law is suspected, CMS will notify the Office of the Inspector General's (OIG) Computer Crime Unit and submit a report to the FedCIRC of the incident with a copy to the CMS Senior Information Systems Security Office.

As part of the risk management process, the business partner should determine the extent of the incident's impact and the potential for new or enhanced controls required to mitigate newly identified threats. These new security controls (and associated threats and impacts) should provide additional input into the business partner's risk assessment. Business partners *should* refer to The CMS System Security Incident Handling Procedures for further guidance. This

document can be found at *http://www.cms.hhs.gov/InformationSecurity/15_Procedures.asp#TopOfPage*.

3.7 - System Security Profile

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed CISS Self Assessments
- *S*ystem Security Plan (for each GSS and MA)
- *R*isk Assessments
- *C*ertifications
- *I*T Systems Contingency Plans
- ACA Reports *(No longer required as of October 1, 2006)*
- POA&Ms for each *compliance* security review
- *POA&Ms for other s*ecurity review undertaken by DHHS OIG, CMS, IRS, GAO, consultants, subcontractors, and business partner security staff
- *Incident reporting and responses*
- Systems security policies and procedures

The System Security Profile shall be kept in a secure location, *kept* up-to-date, and pointers to other relevant documents *maintained*. *A* backup copy of the System Security Profile *shall be kept at a secure off-site storage location,* preferably at the site where back-up tapes and/or back-up facilities are located. *The* back-up copy of the profile *shall also be kept* up-to-date, particularly the contingency plan *documents*.

3.8 - Fraud Control

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partners are required to safeguard systems against fraud. The CMS CSRs address fraud control issues such as personnel screening, separation of duties, rotation of duties, and training. Business partners should practice fraud control in accordance with Appendix A, *the* CISS and the CMS CSRs, and Appendix C, An Approach to Fraud Control.

3.9 - Patch Management

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Timely patching is critical to maintaining the operational availability, confidentiality, and integrity of Medicare systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily and it is often difficult for even experienced system administrators to keep abreast of all the new patches. *The* CERT/Coordination Center (CC) (*http://www.cert.org*) estimates that 95 percent of all network intrusions could be avoided by keeping systems up-to-date with appropriate patches.

To help address this growing problem, CMS recommends that business partners have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. The CSRs provide specific guidance on time frames for implementation of patches.

NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*, provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS highly encourages business partners to utilize NIST and other guidance documents to develop configuration standards, templates, and management processes that securely configure Medicare systems as part of their configuration management program.

3.10 - Security Management Resources

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

3.10.1 - Security Configuration Management

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government.

CMS security configuration management guidance, including DHHS requirements and links to NIST, NSA, and DISA configuration guides are provided in Appendix F.

CMS does not require the verbatim use of these guidance documents and tools for the configuration of Medicare systems. However, CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity. CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

NOTE: DMEMACs, ABMACs, and EDCs are required to start with these Security Technical Implementation Guide (STIG) baseline configurations and then document any exceptions based on environment specific implementation.

3.10.2 - National Institute of Standards and Technology (NIST)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards Publications (FIPS), Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-XX) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, references to the "waiver process" contained in many of the FIPS are no longer operative. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST *Special P*ublications for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are incorporated into the *CMS BPSSM and the* CMS CSRs. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Table 3.*2* contains a listing of NIST publications relevant to common systems or technology utilized within the Medicare business partner community. Table 3.*2* is not meant to be all-inclusive and may contain some references that are not applicable to a particular Medicare business partner application. The most current NIST publications can be found at http://csrc.nist.gov/publications/index.html.

Table 3.*2*. NIST Publications

Publication Number	Title
SP 800-103 (Draft)	*An Ontology of Identity Credentials, Part I: Background and Formulation*
SP 800-101 (Draft)	*Guidelines on Cell Phone Forensics*
SP 800-100	*Information Security Handbook: A Guide for Managers*
SP 800-98 (Draft)	*Guidance for Securing Radio Frequency Identification (RFID) Systems*
SP 800-97 (Draft)	*Guide to IEEE 802.11i: Robust Security Networks*
SP 800-96	*Personal Identity Verification (PIV) Card / Reader*

Publication Number	Title
	Interoperability Guidelines
SP 800-95 (Draft)	*Guide to Secure Web Services*
SP 800-94 (Draft)	*Guide to Intrusion Detection and Prevention (IDP) Systems*
SP 800-92	*Guide to Computer Security Log Management*
SP 800-90	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
SP 800-*89* (Draft)	*Recommendation for Obtaining Assurances for Digital Signature Applications*
SP 800-*88*	*Guidelines for Media Sanitization*
SP 800-*86*	Guide to *Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*
SP 800-*85A*	*PIV Middleware and PIV Card Application Conformance Test Guidelines*
SP 800-85B	*PIV Data Model Conformance Test Guidelines*
SP 800-*84*	*Guide to Single-Organization IT Exercises (Withdrawn pending update)*
SP 800-83	*Guide to Malware Incident Prevention and Handling*
SP 800-82	*Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*
SP 800-81	*Secure Domain Name System (DNS) Deployment Guide*
SP 800-80 (Draft)	*Guide for Developing Performance Metrics for Information Security*
SP 800-79	*Guidelines for the C&A of PIV Card Issuing Organizations*
SP 800-78-1 (Draft)	*Cryptographic Standards and Key Sizes for PIV*
SP 800-78	*Cryptographic Algorithms and Key Sizes for PIV*
SP 800-77	*Guide to IPsec VPNs*
SP 800-76	*Biometric Data Specification for PIV*
SP 800-73 Rev. 1	*Interfaces for PIV*
SP 800-72	Guidelines on PDA Forensics
SP 800-70	*Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-64 *Rev. 1*	Security Considerations in the Information System Development Life Cycle
SP 800-63 *Rev. 1.0.2*	Electronic Authentication Guideline: Recommendations of the *NIST*

Publication Number	Title
SP 800-61	Computer Security Incident Handling Guide
SP 800-60 *Vols. 1&2*	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-58	Security Considerations for Voice Over IP (VoIP) Systems
SP 800-57	Recommendation on Key Management
SP 800-*56A*	Recommendation *for Pair-Wise* Key *Establishment Schemes Using Discrete Logarithm Cryptography*
SP 800-55	Security Metrics Guide for *IT* Systems
SP 800-53A	*Guide for Assessing the Security Controls in Federal Information Systems*
SP 800-53 *Rev. 1*	Recommended Security Controls for Federal Information Systems
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-50	Building an *IT* Security Awareness and Training Program
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-47	Security Guide for Interconnecting *IT* Systems
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Windows 2000 Professional
SP 800-42	Guideline on Network Security Testing
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-40 *Ver. 2*	*Creating a Patch and Vulnerability Management Program*
SP 800-37	Guide for the Security C*&A* of Federal Information Systems
SP 800-36	Guide to Selecting Information Security Products
SP 800-35	Guide to *IT* Security Services
SP 800-34	Contingency Planning Guide for *IT* Systems
SP 800-33	Underlying Technical Models for *IT* Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-31	Intrusion Detection Systems (IDS)
SP 800-30	Risk Management Guide for *IT* Systems
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-27 Rev. A	Engineering Principles for *IT* Security (A Baseline for Achieving Security)
SP 800-26 *Rev. 1*	*Guide for Information Security Program Assessments and*

Publication Number	Title
	System Reporting Form
SP 800-25	Federal Agency Use of *PKI* for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21*-1*	Guideline for Implementing Cryptography in the Federal Government
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-19	Mobile Agent Security
SP 800-18 *Rev. 1*	Guide for Developing Security Plans for *IT* Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-16	*IT* Security Training Requirements: A Role- and Performance-Based Model
SP 800-15 *Ver. 1*	Minimum Interoperability Specification for PKI Components (MISPC)
SP 800-14	Generally Accepted Principles and Practices for Securing *IT* Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook
FIPS 201*-1*	*Personal Identity Verification (PIV)* for Federal Employees and *Contractors*
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Advanced Encryption Standard
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 191	Guideline for The Analysis of *LAN* Security
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 188	Standard Security Labels for Information Transfer
FIPS 186-2	Digital Signature Standard (DSS)
FIPS 185	Escrowed Encryption Standard
FIPS 181	Automated Password Generator
FIPS 180-2	Secure Hash Standard (SHS)

Publication Number	Title
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 113	Computer Data Authentication

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

4.0 - IT Systems Sensitivity/Criticality Determinations

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The systems *and information* security efforts of the CMS Business Partner Security Program are based on the *FIPS Pub 199 security categorization standards established for information and information systems. FIPS Pub 199 security categorization is established based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.*

4.1 - *Security Impact Levels*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

FIPS Pub 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems (including contractor systems used to process, store, and/or transmit such information) for each of three security objectives (confidentiality, integrity, and availability). Table 4.1 summarizes the three FIPS Pub 199 security impact levels.

Table 4.1. Security Impact Levels

Potential Impact	***Description***	***Amplification***
Low	*The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.*	*The loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.*

Potential Impact	Description	Amplification
Moderate	*The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*	*The loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.*
High	*The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*	*The loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.*

4.1.1 - *Security Objective Potential Impact Levels*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The security categorization of all CMS information and information systems is based on the FISMA security objectives of confidentiality, integrity, and availability; and the FIPS Pub 199 three levels of potential impact on CMS operations and assets should there be a breach of security (i.e., loss of confidentiality, integrity, or availability). Table 4.2 summarizes the security objectives (i.e., confidentiality, integrity, and availability) of all CMS information and information systems, and the potential impact level definitions for each of the three security objectives.

Table 4.2. Security Objective Potential Impact Definitions

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.* *[44 U.S.C., SEC. 3542]*	*The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.*	*The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*	*The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*
Integrity *Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.* *[44 U.S.C., SEC. 3542]*	*The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.*	*The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*	*The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*
Availability *Ensuring timely and reliable access to and use of information.* *[44 U.S.C., SEC. 3542]*	*The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.*	*The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*	*The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*

4.1.1.1 - Level 1: Low Sensitivity

(Rev. 3, 03-28-03)

This category identifies data that requires minimal protection. Threats to this data are minimal, and only minimal precautions to protect the data need to be taken. Unintentional alteration or destruction is the primary concern for this type of data. This category includes any of the following:

Data only in its raw form, such as in some laboratory research applications, and the computerized correspondence and documents in some offices.

Automated Systems of Records, which contain information that is virtually in the public domain, such as employee locator files, and for which any unauthorized disclosures could be expected not to adversely affect the individual.

4.1.1.2 - Level 2: Moderate Sensitivity

(Rev. 3, 03-28-03)

This category identifies data that has importance to CMS and its business partners, and which must be protected against such acts as malicious destruction. However, because this type of data is most often collected for analytical purposes, disclosure problems are not usually significant. This category includes any of the following:

Management information concerning workload, performance, staffing, and similar data, usually in statistical form, which is used to generate reports that reflect the status of an organization. Access to this data needs to be restricted only to a limited degree. The data is protected because of its value to the organization but is intended for disclosure in some form eventually.

Research and statistical data accumulated to provide information about CMS programs to the public. This data needs protection commensurate with the value of the information to the organization. Loss of this kind of data would not normally be potentially embarrassing or detrimental either to an individual or to the organization.

Automated systems of records subject to the Privacy Act, which contain information not in the public domain, but for which unauthorized disclosure could cause nonspecific embarrassment to an individual.

Computerized correspondence and documents, which must be protected from unauthorized alteration or disclosure. These types of data include all correspondence, memoranda, and other documents whose release or distribution outside the Federal government or within the organization needs to be controlled.

4.1.1.3 - Level 3: High Sensitivity

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This category identifies the most sensitive unclassified data processed within CMS and business partner IT systems. This category of data is referred to as sensitive information within the CMS

CSRs. Data in this category requires the most stringent and the greatest number of information security safeguards at the user level. This category includes, but is not limited to, the following:

- Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

- Any data that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act (FOIA).

- All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the FOIA; i.e., for which unauthorized disclosure would constitute a “clearly unwarranted invasion of personal privacy” likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing. This data includes, but is not limited to, FTI, including all Federal Tax Return information.

- All electronic health care information and individually identifiable health care information as specified in the regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Payment information that is used to authorize or make cash payments to individuals or organizations. This data is usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter to cause an improper payment.

- Medicare proprietary information that has value in and of itself, and which must be protected from unauthorized disclosure.

- Computerized correspondence and documents that are considered highly sensitive or critical to an organization and which must be protected from unauthorized alteration or premature disclosure.

Proprietary information that has value in and of itself and that must be protected from unauthorized disclosure.

4.1.1.4 - Level 4: High Sensitivity and National Security Interest
(Rev. 3, 03-28-03)

The CMS currently processes no information in this category. This category identifies all databases that contain national security classified information and all databases that contain other sensitive but unclassified information, the loss of which could adversely affect national security interests.

4.1.2 - *CMS Information and Information Systems Security Levels*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

CMS has established the security level designation for all information processed, stored, and/or transmitted on business partner and sub-contractor Medicare claims-related information systems at a "HIGH" security level. Business partner System Owners/Managers and System Maintainers/Developers must ensure that their databases and the processing capabilities of their systems are accessed only by authorized users who fully use the required security-level safeguards. The business partner managers of compartmentalized systems must take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The security level designation determines the minimum security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities.

The "HIGH" security level designation applies to both user information and system information, and it is applicable to information in either electronic or non-electronic form. System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at the same level to ensure information and information system confidentiality, integrity, and availability.

4.1.2.1 - Level 1: Low Criticality

(Rev. 3, 03-28-03)

This category identifies systems with data processing capabilities that require minimal protection. These include systems that, in the event of alteration or failure, would affect the organization minimally or could be replaced with minimal staff time or expense. This category also includes systems that generate, store, process, transfer, or communicate data that is considered to have low or no sensitivity (Level 1).

4.1.2.2 - Level 2: Moderate Criticality

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This category identifies systems with data processing capabilities that are considered important but not critical to the internal management of CMS. This category includes the following:

- Systems in which failure to function for an extended period of time would not have a critical impact on the organizations they support.

Systems that generate, store, process, transfer, or communicate data that is considered to have moderate sensitivity (Level 2).

4.1.2.3 - Level 3: High Criticality
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This category identifies systems with data processing capabilities that are considered critical to CMS. This category includes the following:

- Systems whose failure to function for even a short period of time could have a severe impact on CMS or the organizations that they support.

- Systems that perform functions with data that are considered to have a high potential for fraud, waste, or abuse.

Systems that generate, store, process, transfer, or communicate data that is considered to have high sensitivity (Level 3) and categorized as sensitive information.

4.1.2.4 - Level 4: High Criticality and National Security Interest
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This category identifies all systems with data processing capabilities that are considered critical to the well being of the CMS organization. An example would be systems that handle sensitive-but-unclassified information, the loss of which could adversely affect national security interests. National security directives and other Federal government directives require that these systems be protected in proportion to the threat of compromise or exploitation and the associated potential damage to the interest of CMS, its customers, and personnel.

4.1.3 - Criticality Impact Levels for IT Systems
(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

There are no separate criticality impact levels for IT information systems. The FIPS Pub 199 security categorization is established based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Therefore, the criticality level is considered when the security impact category is established.

4.2 - *CMS Sensitive Information Protection Requirements*
(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Business partners are responsible for implementing a Minimum Protection Standard (MPS) for all *information categorized at a "HIGH" security level* (*i.e.,* CMS sensitive) information and materials. The MPS applies to all IT facilities, areas, or systems processing*,* storing*, or transmitting* CMS sensitive information in any form or on any media. The following *table* should be used to determine the minimum standards required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The following alternative methods are not listed in any order of preference or security significance.

Table 4.*3*. Protection Alternative Chart

	Perimeter Type	Interior Area Type	Container Type
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		Secur*ed*

Because local factors may require additional security measures, management must analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS has been designed to provide management with a basic framework of minimum security requirements.

The objective of these standards is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security:

Alternative #1: secured perimeter and locked container

Alternative #2: locked perimeter and secured interior

Alternative #3: locked perimeter and secur*ed* container

"Locked" means a perimeter, area, or container that has both a lock and keys or combinations that are controlled. A secur*ed* container is a lockable metal container with a resistance to forced penetration, with both a security lock and keys or combinations that are controlled. (See the following sections for additional explanation and details on these requirements.)

The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information must be containerized in areas where other than authorized employees may have access after hours (e.g., security personnel or custodial service personnel).

4.2.1 - *Restricted Area*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A restricted area is *a secured area* whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas must either meet secured area criteria or provisions must be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information.
Restricted areas will be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance must have controlled access (electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

4.2.2 - Security Room
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (normal construction material, permanent in nature, such as masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room must be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking Systems for Secured Areas and Security Rooms).

Additionally, any glass in doors or walls will be security glass [at least two layers of 1/8-inch plate glass with .060-inch (1/32) vinyl interlayer, nominal thickness shall be 5/16-inch]. Plastic glazing material is not acceptable. Vents and louvers will be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that will annunciate at a protection console, UL-approved central station, or local police station; it will be given top priority for guard/police response during any alarm situation.

Cleaning and maintenance should be performed in the presence of an employee authorized to enter the room.

4.2.3 - Secured Interior/Secured Perimeter
(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Secured areas are *perimeter and/or interior areas which* have been designed to prevent undetected entry by unauthorized persons during non-working hours. *To qualify as a secured area, the space or perimeter* must meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser-type partition (i.e., slab-to-slab walls) supplemented by UL-approved electronic IDS and fire detection systems.

- Unless electronic IDS devices are used, all doors entering the space must be locked, and strict key or combination control should be exercised.

- In the case of a fence and gate, the fence must have IDS devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms.

The space must be cleaned during working hours in the presence of a regularly assigned employee.

4.2.4 - Container
(Rev. 4, 03-05-04)

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, and any other piece of office

equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 - Locked Container
(Rev. 4, 03-05-04)

Locked containers must include lock mechanisms that use either a built-in key, or hasp and lock, and include the following features: (1) metal cabinet or box with riveted or welded seams, or (2) metal desks with locking drawers.

4.2.4.2 - Security Container
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. Combinations for combination locks will be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks
- Key lock “Mini Safes” properly mounted with appropriate key control.

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

4.2.4.3 - Safes/Vaults
(Rev. 4, 03-05-04)

A safe/vault is not required for storage of CMS sensitive information. However, if one is used for such storage, it must be located within a secured or locked perimeter type and it must meet the following requirements:

- A safe is a GSA-approved container of Class 1, IV, or V, or UL listings of TRTL-30, TXTL-60, or TRTL-60.
- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, that uses UL-approved vault doors and meets GSA specifications.

4.2.5 - Locking Systems for Secured Areas and Security Rooms
(Rev. 4, 03-05-04)

Minimum requirements for locking systems for Secured Areas and Security Rooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock.
- Have a deadbolt throw of one inch or longer.
- Double-cylinder design. Cylinders are to have five or more pin tumblers.
- If bolt is visible when locked, it must contain hardened inserts or be made of steel.
- Both key and lock must be "off-master."
- Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours.
- Keys to secured areas not in the personal custody of an authorized employee and all combinations will be stored in a security container.

4.2.6 - Intrusion Detection System (IDS)

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

Physical Intrusion Detection Systems are designed to detect attempted perimeter area breaches. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection during non-working hours. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, and are designed to set off an alarm at a given location when the sensor is disturbed.

5.0 - Internet Security

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

Transmission of and/or receipt of health care transactions (claims, remittances, etc.) or other CMS sensitive data over the Internet is prohibited at Medicare business partners (or their agents). Practically, this prohibition means that CMS requires the use of private networks or dial-up connections with any entity that transmits or receives health care transactions and/or CMS sensitive data to or from the Medicare contractor. CMS is closely following the health care industry's movement toward adoption of industry-wide security technologies that ensure confidentiality, integrity, and availability of data moved over the Internet and will reconsider its policy at the appropriate time.

Appendix A:
The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs)

Table of Contents
(Rev. 7, 03-17-06)

1.0 - Introduction to the CMS Integrated Security Suite (CISS)
(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Each Business Partner is required to provide input into the CISS as directed by CMS in support of CMS security objectives. Findings from internal/external audits (once approved by CMS) /reviews/self assessments are entered into the CISS. Only findings from CMS-initiated audits (e.g., Section 912 Evaluation or Testing, Chief Financial Officer [CFO], Statement on Auditing Standards No. 70 [SAS 70]) require CMS concurrence or approval before they should be entered into the CISS. These all involve the establishment of Weakness records and Action Plans. Weakness and Action Plan records resulting from these are linked together with other appropriate CISS data. This information becomes part of the monthly POA&M package as directed in section 3.5.2 of the BPSSM.

The mechanics of CISS use are provided in the CISS User Guide, while guidance for populating specific fields is provided in this appendix. The CISS is available for download on the CMS Web site.

2.0 - CISS Self-Assessment (CAST) Module
(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Self-Assessment module in the CISS functions similarly to the former standalone CMS Contractor Assessment Security Tool (CAST). Business Partner designees enter text responses to each Core Security Requirement (CSR)—see Attachment A—indicating the Business Partner's level of compliance with CMS security requirements. In this manner, CMS Business Partners are able to perform their required annual systems security Self-Assessments.

The CISS also assists the Business Partner by validating and preparing the Self-Assessment data file for submission to CMS as part of its annual certification material. The CISS Self-Assessment module provides Business Partners with a powerful reporting tool that generates formatted Self-Assessment forms, copies of CMS CSRs, and standardized reports.

Business *P*artners must complete the CISS Self-Assessment and submit *a separate* copy *for each contract type (i.e. data center, fiscal intermediary, carrier, program safeguard contractor, standard system maintainer, Medicare Administrative Contractor, coordination of benefits, etc.)* on CD-ROM to both the CMS Central Office and the Consortium Contractor Management Officer (CCMO) for Title XVIII contracts or the Project Officer (PO) for Federal Acquisition Regulation (FAR) contracts by close of business April 2*7*, 200*7*. Be advised that this information must not be submitted to CMS via email. Registered mail or its equivalent should be used. Should you need technical assistance, contact the CMS/Northrop Grumman Help Desk at 703-*272-5725*.

The completed Self-Assessment must be included in the Security Profile (see section 3.7 of the BPSSM). Business Partners may also use the CISS to conduct Self-Assessments in preparation for audits by specific external entities such as the Government Accounting Office (GAO), Internal Revenue Service (IRS), Department of Health and Human Services (DHHS) Office of Inspector General (OIG), and CMS. The CISS allows the Business Partner to generate a

worksheet consisting of those CSRs and Protocols that have a particular source document as a reference (e.g., IRS Pub 1075, NIST, FISCAM,).

Instructions for using the CISS are contained in the CISS User Guide, which is available in the application itself by clicking on the Help link at the top of the main menu.

2.1 - Applicable Laws

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

CMS CSRs detail technical requirements for CMS Business Partners who use information systems to process Medicare data. Business *P*artner s must establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data.

The CMS CSRs are developed by assessing and analyzing requirement statements from a number of Federal and CMS mandates, including the following:

- Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- OMB Circular No. A-127, Financial Management Systems, June 21, 1995.
  http://www.whitehouse.gov/omb/circulars/index.html

- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999.
  http://www.whitehouse.gov/omb/circulars/a127transmittal2.html

- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000.
  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000.
  http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

- Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources, *Memorandum, July 17, 2004.*
  http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf

- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999.
  http://www.gao.gov/special.pubs/12_19_6.pdf

- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.

http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

- CMS System Security Plans (SSP) Methodology, Draft Version 3.0, November 6, 2002. *http://www.cms.hhs.gov/InformationSecurity/Downloads/ssp_meth.pdf*

- CMS Information Security Risk Assessment Methodology, Version 2.1, April 22, 2005. *http://www.cms.hhs.gov/InformationSecurity/Downloads/RA_meth.pdf*

- CMS Information Security Acceptable Risk Safeguards (ARS), Version 2.*0*, *March 13, 2006*.
  http://www.cms.hhs.gov/it/security/References/ps.asp

- IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, June 2000.
  http://www.irs.gov/pub/irs-pdf/p1075.pdf

- Health Insurance Portability and Accountability Act (HIPAA), August 21, 1996.
  http://aspe.os.dhhs.gov/admnsimp/pl104191.htm
  http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm

2.2 - CSR Categories

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

CMS has organized the CSRs into Categories. There are ten Categories comprising six general Categories, three application Categories, and an additional Category, "Network." The ten Categories are as follows:

Category	Description
Entity-wide Security Program Planning and Management	These controls address the planning and management of an entity's control structure.
Access Control	These controls provide reasonable assurance that information-handling resources are protected against unauthorized loss, modification, disclosure, and damage. Access controls can be logical or physical.
System Software	These controls address access and modification of system software. System software is vulnerable to unauthorized change and this Category contains critical elements necessary for providing needed protection.
Segregation of Duties	These controls describe how work responsibilities are segregated so that one person does not have access to or control over all of the critical stages of an information handling process.
Service Continuity	These controls address the means by which the entity attempts to ensure continuity of service. A Business Partner cannot lose its capability to process, handle, and protect the information it is entrusted with.

Category	Description
Application Software Development and Change Control	These controls address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information (FTI).
Application System Authorization Controls	These controls address the processing of Medicare data in a manner that ensures that only authorized transactions are entered into the information processing system.
Application System Completeness Controls	These controls ensure that all system transactions are processed and that any missing or duplicate transactions are identified and a remedy implemented.
Application System Accuracy Controls	These controls address the accuracy of all data entered into systems for processing, handing, and storage. Data must be valid and accurate. All invalid, erroneous, or inaccurate data must be identified and corrected.
Network	These controls address the network(s) structure. The network structure must be protected and the data transmitted on the networks must be protected.

Table A-1. CSR Category Descriptions

2.3 - CSR Elements

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Each Category is further organized into General Requirements and Control Techniques. Protocols, Guidance, References, Related CSRs, and Applicable Types are additional CSR elements that are included with each CSR for interpretive and application purposes. Table A-2 below shows the relationship among the CSR elements (General Requirements, Control Techniques, Protocols, Guidance, References, and Related CSRs).

Table A-2. CSR Elements

Category: 1. Entitywide Security Program Planning and Management		
General Requirement: 1.1. Management and staff shall receive security training, security awareness, and have security expertise.		
Control Technique:	**Protocol(s):**	**Reference(s):**

1.1.1. Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).	Review the training policy. Interview a sample of site personnel to verify that documented training was received. Review documented procedure for generation of security reminders. Review a sample of training records to confirm completion of the required training. Review training syllabus for inclusion of the required training.	NIST 800-53: AT-2 NIST 800-53: AT-3 HIPAA: 164.308(a)(5)(i) HIPAA: 164.308(a)(5)(ii)(A) HIPAA: 164.308(a)(5)(ii)(B) HIPAA: 164.308(a)(5)(ii)(C) HIPAA: 164.308(a)(5)(ii)(D) ARS: AT-3.2 ARS: AT-2.3 FISCAM: TSP-4.2.2
	Guidance: A formal program should be established with a policy and a procedure.	**Related CSR(s):** 2.9.2, 5.12.1
Applicable Types: COB, CWF, DC, *EDC, ABMAC*, PartA, PartB, PSC, SS, *DME*MAC		

General Requirements define elements of systems or operations that must be safeguarded. The example above shows General Requirement 1.1 from the Category 1, Entitywide Security Program Planning and Management. The General Requirement states, "Management and staff shall receive security training, security awareness, and have security expertise."

Control Techniques describe particular system elements that must be in place to consider the General Requirement to be in compliance. The example above shows Control Technique (or CSR) 1.1.1, which states, "Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential)." A Business Partner would be in compliance with Control Technique (or CSR) 1.1.1 when all control elements listed in the CSR are in place.

To assist Business Partners in the development of CSR responses, CMS has developed additional information to clarify common CSR issues:

Protocols. *P*rocedures designed to verify that a*n entity* is in compliance with system security requirements. Protocols have been developed based on the same Federal and CMS security documents used to create the CSRs. As such, they provide Business Partners with Self-Assessment procedures*, specific to each CSR,* that are similar to audit procedures used by CMS and external *auditing* agencies. *Further, it is required that the associated protocols be used by Business Partners for testing/validation of CSRs before the applicable CSR can be considered Level 4 (L4) compliant*. *Protocol* information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.

Guidance. Additional clarifying information regarding each CSR. This information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.

References. Source documents and section or paragraph designators from which one or more CSR control techniques were extracted. Because CMS CSRs have retained their source references, Business Partners can conduct "modular" Self-Assessments that address the likely audit procedures that would be used by an external agency. For example, to prepare for an audit by the IRS, or to perform a preparatory Self-Assessment, a Business Partner SSO might review the CSRs specifically associated with IRS Pub 1075. Additionally, the SSO could use references in the CISS database to determine the location of a requirement in IRS Pub 1075. This information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.

Related CSRs. Each CSR may be related to one or more other CSRs. It may be important for certain CSR responses to be coordinated with related CSRs. At the very least, Business Partners should take care to ensure that related CSR responses do not conflict. This information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.

Applicable Contract Types. The likely contract types to which a CSR applies (refer to the legend below). Developed jointly by CMS and Business Partner security experts, the Applicability list is not meant to be used as a requirements document; however, it does give Business Partners and CMS reviewers an initial indication of whether a particular CSR should be addressed by a given Business Partner. This information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.

Applicability legend:

COB – Coordination of Benefits
CWF – Common Working File [Host]
DC – Data Center
DMEMAC - Durable Medical Equipment *Medicare Administrative Contractor*
PartA – Part A Fiscal Intermediary
PartB – Part B Carrier
PSC – Program Safeguard Contractor
SS – Standard System [Maintainer]
*AB*MAC – *A/B* Medicare Administrative Contractor
EDC – Enterprise Data Center

CMS continues to focus on protecting the health information received from its beneficiaries while processing claims.

Ensuring the confidentiality, integrity, and availability (CIA) of CMS sensitive information remains of paramount concern in the continuing effort to improve the overall security program. CMS continues to review evolving Federal security standards and directives to ensure that the CMS CSRs are current and compliant with all Federal mandates. CMS has provided technical clarifications and accounted for the potential impacts of any updated or new requirements. The following rationales are used in preparing these modifications:

- Where Federal improvements are already covered by an existing CSR, these documents are added as references.

- Where Federal improvements are partially covered by an existing CSR, the existing CSR is modified to incorporate appropriate language and the appropriate document(s) are listed as reference(s).

- Where Federal improvements are not covered by an existing CSR, a new CSR is added and the appropriate document(s) are listed as a reference(s).

At the present time, CMS does not anticipate any additional funding being provided to Business Partners to address any new requirements. Any new requirements represent best practices, and CMS believes many contractors are already compliant or in the process of implementing changes to become compliant.

Where the implementation of alternatives and/or compensating controls is not possible, a contractor's non-compliance must also be documented in the Risk Assessment (RA), System Security Plan (SSP), and the CISS Self-Assessment. CMS encourages Business Partners to fund these requirements by reallocating/reprogramming current fiscal year resources. CMS also recognizes that there are times when controls cannot be implemented due to resource issues. Alternative or compensating safeguards can be implemented to reduce the risks to CMS and its systems. This must be considered part of risk management and the alternative or compensating controls must be documented in the information security risk assessment, SSP, and annual CISS Self-Assessment submissions.

2.4 - Completing the Self-Assessment (CAST)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The CISS Self-Assessment (CAST) form is where Business Partners indicate their compliance with each CSR. Business *P*artners select a Status, and provide a descriptive text response that provides details of the Status marked for that CSR.

2.5 - All Responses

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The following information and guidance should be considered when evaluating all CSRs and preparing CSR responses:

a) When entering information into the CISS Self-Assessment, the Business Partner shall provide specific information in the Response Comment/Explanation field as to the status of compliance with the applicable requirement. The CISS can then produce a pre-formatted report of Self-Assessment results along with graphical analysis.

b) Each CSR requires a Status (i.e., “Level 0,” “Level 1,” “Level 2,” “Level 3,” “Level 4,” “Level 5,” or “N/A”) to be selected, and each CSR requires a detailed explanation in the

Response Comment/Explanation field to describe and explain the compliance status. In addition, all CSR responses must include a complete description of What, Where, Why, and How each CSR is or is not in compliance, depending on the CSR status selection.

c) Every CSR response requires that a principle Point-of-Contact (POC) be designated. The CISS provides a specific field for this information, and the field requires that at least one POC value be entered. Other interested POCs may also be assigned to a CSR as non-primary designees. However, one and only one *p*rimary POC must be assigned to each CSR response.

d) Business *P*artners should be aware that even if data processing duties are subcontracted out to either another CMS Business Partner (such as a data center) or to a third-party subcontractor (such as a business services company), responsibility for the implementation of security controls ultimately resides with the primary contract holder. Business *P*artners should coordinate the establishment of boundaries for specific issues. While this does not necessarily require a sharing of Self-Assessment responses, it does require that Business Partners communicate and coordinate among themselves such that interfaces of responsibilities for particular CSRs are addressed by all responsible entities without gaps in coverage.

e) Where a merging of responsibilities occurs among Business Partners (such as the interface between data centers, claims processors, and standard system maintainers), a detailed description of these interfaces and the division of responsibilities should be provided in the Response Comment/Explanation field. The description should include local responsibilities as well as those that are perceived to be responsibilities of some other CMS Business Partner.

f) Each CSR in the CISS includes an Applicability matrix, which identifies the likely responsibility for each CSR by CMS contract type (e.g.., Part A, Part B, *CWF*). The purpose of the Applicability matrix is not to summarily include or exclude CSRs from a particular contract type. The Applicability matrix is designed to be used as a guide to Business Partners. CMS recognizes that system configurations vary widely throughout the Business Partner community; therefore, each Business Partner must evaluate and report on each CSR's applicability to its own systems.

g) Business *P*artners should also be aware of the CSR terms included in the BPSSM Glossary (Appendix *H*) and address the CSRs as they apply to their local environment. For example, the term "data center" refers to any site or location where information is processed (e.g., claims entry and processing) and is not limited to a CMS or Business Partner "Data Center" (e.g., mainframe environment). A "system" may include mainframe systems, desktop systems, workstations and servers, networks, and any platform regardless of the operating system. "System software" includes the operating system and utility programs (e.g., workstation, server, and network software and utilities) and is distinguished from application software. "Application software" includes the standard system (i.e., Major Application) but it also includes any computer program (i.e., application) that manipulates data or performs a specific function (e.g., front-end and back-end applications).

h) If corporate policy conflicts with a CMS CSR, a detailed explanation must be provided as to why the corporate policy cannot be modified to apply to CMS data. Any conflicts with corporate policy (in which the final disposition of the CSR response would not ultimately result in full compliance with CMS requirements) must be addressed for resolution, by written correspondence with the CMS Central Office, prior to indicating such in any CSR response.

Business *P*artners are required to enter a current status and a detailed Comment/Explanation for each CSR. The annual Self-Assessment is one of the central documents in the Business Partner's security profile and should reflect sufficient detail to convey to CMS the current status of the Business Partner's security program. The decision tree in Figure A-1 has been developed to assist in the establishment of the current status of the Business Partner security.

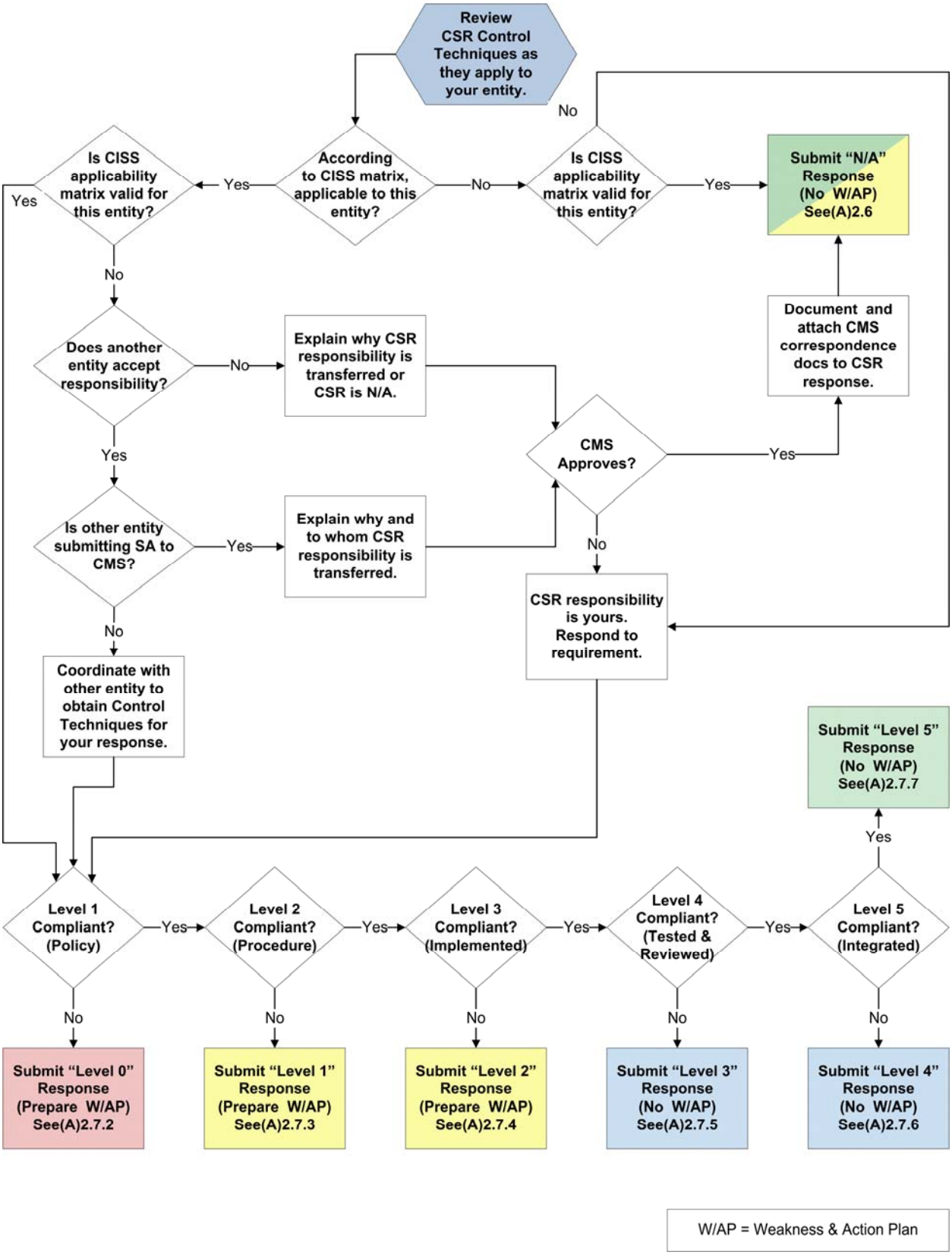

Figure A-1. Response Status Decision Tree

2.6 - "N/A" Response Status

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A response status of "N/A" indicates that the Control Technique requirements are not applicable to this entity. CMS expects most, if not all, CSRs to apply to all portions of all Business Partner contracts. Very few CSRs are expected to receive "N/A" responses. The Response Comment/Explanation field should contain a detailed explanation of the circumstances that render this CSR non-applicable (regardless of whether this CSR is listed as applicable in applicability matrix for a particular contract type), and how this information can be verified, in a format that clearly answers each question described below:

a) **Why** is this CSR not applicable?

A complete and detailed description should be provided to describe the circumstances that render the subject CSR "N/A" to a particular Business Partner. Referral to the Applicability matrix is NOT sufficient justification for an "N/A" response. A full understanding of the reasons for non-applicability must be demonstrated and explained in the CSR response. This is because the Applicability matrix is not definitive, and CMS anticipates cases in which a CSR will indeed apply to one or more entities even when the CISS Applicability matrix indicates it generally does not. Note that CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability list.

b) **How** did you verify this status with CMS?

i. **Applicability matrix says CSR is NOT applicable.** CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability matrix.

ii. **Applicability matrix says CSR is applicable.** In the case of an "N/A" response that is not corroborated by the Applicability matrix, CMS approval must be obtained and documented, and such documentation must be provided with the CSR response (see below). Note that CMS approval must be renewed each year for each "N/A" CSR to be waived.

The CISS tool require*s* that copies of the associated CMS approval documentation *are* attached to the CSR response within the CISS tool. Approvals for prior years may be cited in you*r* request for CMS approval for the current year response but cannot be used as documentation of CMS approval for the current year CSR "N/A" response. Each year, the CMS approval process must be repeated (unless specifically stated in the CMS-provided approval documentation).

In addition to the requirements stated above in section *2.6.*a), include the following information with CMS-approved "N/A" responses:

(1) Date CMS approved the response,
(2) CMS office that approved the response, and

(3) Attached documentation of CMS concurrence (e-mail text file, or letter/document).

Example entry for a CMS-approved CSR with a response status of "N/A":

"This requirement describes the required features of 'security rooms.' CSR 2.2.25 suggests 'security rooms' as one of several possible methods, but does not require one. We use 'secured areas' and 'appropriate containers' (CSRs 2.2.19 and 2.2.5). This issue was discussed via letter to CMS (05/15/05) and agreed to by the CMS (06/80/05). Both letters are attached to this CSR response and are on file in cabinet #3 in the Security Office located on the third floor of Bldg. #3."

2.7 - Five Levels of Security Effectiveness

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The 5-Levels of Security Effectiveness are described in NIST publications. Level 1 reflects that a system has a documented security policy. At Level 2, the system also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At Level 5, the system has procedures and controls fully integrated into a comprehensive program. Each level represents a more complete and effective security program.

Level 0	None of the 5-Levels have been addressed
Level 1	Documented Policy
Level 2	Level 1 and Documented Procedures
Level 3	Level 2 and Implemented Procedures and Controls
Level 4	Level 3 and Tested and Reviewed Procedures and Controls
Level 5	Level 4 and Fully Integrated Procedures and Controls

Table A-3. Levels of Security Effectiveness

Since the five levels represent a measure of the maturity of the security function of a system, there is a hierarchical and dependent relationship between each of the Levels of Effectiveness. For example, if a security control is implemented (as in Level 3) but there is no formal policy in place requiring that the control be implemented (as in Level 1), then that CSR status is considered to be at Level 0. A CSR status cannot proceed to the next Level of Effectiveness until all of the previous lower levels have been fully achieved.

a.) **Weaknesses.** Currently, each CSR must minimally be at Level 3 (or above) to be considered in compliance. For any response at Level 2 or below, the [Weakness] button on the CISS Self-Assessment form is enabled. An appropriate Weakness/Action Plan combination must accompany any CSR response at Level 2 or below. However, CMS does not consider a CSR response to be at full maturity until Level 5 is achieved. The CMS goal is to "Strive-for-Five."

b.) **Risk-Based Decision**. In some extreme cases, full implementation of the minimum compliance requirements may present unacceptable fiscal or configuration barriers. In these cases, CMS may agree that the risk is acceptable for the present self-assessment and that no Weakness/Action Plan combination is required nor desired. In such cases,

prior CMS concurrence is required AND a full assessment of all of the implications of not meeting each of the minimum 3 levels for the applicable CSR is fully documented in the associated risk-assessment for the system. BOTH the updated risk-assessment AND full documentation of CMS concurrence MUST be attached to the CSR response.

2.7.1 - Response Status (Levels 0, 1, 2, 3, 4, 5)

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Each response level (1 through 5) indicates that all of the CSR requirements up to and including the selected Level are currently being fully met with in-place measures or controls. The Response Comment/Explanation field should, at a minimum, contain a detailed explanation of how the stipulations of the CSR are being met, and how compliance can be verified, in a format that clearly answers each question described below:

a) **What** can be used to verify full compliance?

Verification of CSR compliance is a fundamental part of the Self-Assessment process. Documentation in the form of logs, procedures, manuals, policies, employee training records, must be available to verify compliance. A control that is not verifiable is not normally considered acceptable. The specific document(s) must be named for a response to be considered complete.

b) **Where** can the applicable documentation be found?

Methods of verification should be accessible to auditors. Ensure that the method of access and location of applicable documentation is clearly described. This will ensure that the documentation can be retrieved and accessed easily when needed.

c) **How** exactly is the CSR met?

i. Do not include planned controls or controls that are not fully implemented. If all components are not fully in place, the response status must be changed to the next lower level and, if required, a suitable Weakness/Action Plan combination identified.
ii. In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.

Example entry for a CSR with a response status of Level 3:

"Security Awareness Training policies and procedures are in-place and such training is conducted during initial employee orientation and every year during the month of November for all employees and contractors. It includes all aspects outlined in the CSR as documented in company policy NG 7541-S3 and associated HR procedures T255, T256, and T257. The records of attendance are maintained in cabinet #5 in the Corporate Training Office, on the fifth floor of Bldg. #5."

2.7.2 - "Level 0" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

A response status of Level 0 indicates non-compliance with Level 1 of the requirements of the CSR. Since the 5 levels represent a measure of the maturity of the security function of a system, there is a hierarchical and dependent relationship between each of the Levels of Effectiveness. For example, if a security control is implemented (as in Level 3) but there is no formal policy in place requiring that the control be implemented (as in Level 1), then that CSR status is considered to be at Level 0 (no matter what other Levels of Effectiveness are achieved!). A CSR status cannot proceed to the next Level of Effectiveness until all of the previous lower levels have been fully achieved.

2.7.3 - "Level 1" Response Status

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Level 1 – Policy includes:

- Formally documented and disseminated security policy covering Medicare claims processing facilities, personnel, systems, and applications. The policy may be enterprise, system, or application-specific.

A system is at Level 1 if there is a formal, up-to-date, and documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness. Such a policy may be at an organizational level or Medicare claims processing specific *level*.

A documented security policy is necessary to ensure adequate and cost-effective organizational and system security controls. A sound policy delineates the security management structure and clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance.

2.7.4 - "Level 2" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 2 – Procedures – includes:

- Formal, complete, well-documented procedures for implementing policies established at Level 1.

- The basic requirements and guidance issued from applicable public laws; other Federal, department, and agency policy; as well as applicable NIST publications.

A system is at Level 2 when formally documented procedures are developed that focus on implementing specific security controls. Formal procedures promote the continuity of the security program. Formal procedures also provide the foundation for a clear, accurate, and complete understanding of the program implementation. An understanding of the risks and related results should guide the strength of the control and the corresponding procedures. The procedures document the implementation of and the rigor in which the control is applied. Level 2 requires procedures for a continuing cycle of assessing risk and vulnerabilities, implementing effective security policies, and monitoring effectiveness of the security controls. Approved system security plans are in place for all systems. Well-documented and current security

procedures are necessary to ensure that adequate and cost-effective security controls are implemented.

2.7.5 - "Level 3" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 3 – Implemented – includes:

- Security procedures and controls that are implemented.

- Procedures that are communicated and individuals are required to follow them.

At Level 3, the information security procedures and controls are implemented in a consistent manner and reinforced through awareness and training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for a system could be implemented and not have procedures documented, but the addition of formal documented procedures at Level 2 represents a significant step in the effectiveness of implementing procedures and controls at Level 3. While testing the ongoing effectiveness is not emphasized in Level 3, some testing is needed when initially implementing controls to ensure they are operating as intended.

2.7.6 - "Level 4" Response Status

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Level 4 – Tested includes:

- *Periodically (at least annually) evaluating* the adequacy and effectiveness of security policies, procedures, and controls *using the applicable CSR protocols*.

- Ensuring that effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual security incidents or through security alerts issued by Federal organizations, vendors, and other trusted sources.

Routine assessments and response to identified vulnerabilities are important elements of risk management, which includes identifying, acknowledging, and responding, as appropriate, to changes in risk factors (e.g., computing environment, impact levels) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis.

Routine assessments are an important means of identifying inappropriate or ineffective security procedures and controls, reminding employees of their security-related responsibilities, and demonstrating management's commitment to security. Assessments can be performed by Business Partner staff, contractors, or others engaged by CMS management. Independent audits, such as those arranged by the General Accountability Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for assessments initiated by Business Partner management.

To be effective, routine assessments must include tests and examinations of security controls. Reviews of documentation, walk-through of Business Partner facilities, and interviews with Business Partner personnel, while providing useful information, are not sufficient to ensure that

controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. To be meaningful, assessments should include security controls of interconnected assets (e.g., network supporting applications being tested).

When systems are first implemented or are modified, they should be tested and certified to ensure that the security controls are initially operating as intended. (This would occur at Level 3.) Requirements for subsequent testing and recertification should be integrated into an agency's ongoing test and assessment program.

In addition to test results, Business Partner assessments should consider information gleaned from records of potential and actual security incidents and from security alerts, such as those issued by software vendors. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risks.

2.7.7 - "Level 5" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 5 – Integrated – includes:

- A comprehensive security program that is an integral part of a Business Partner's organizational culture.

- Decision-making based on cost, risk, and mission impact.

The consideration of information security is pervasive in the culture of a Level 5 system. A proven life-cycle methodology is implemented and enforced, and an ongoing program to identify and institutionalize best practices has been implemented. There is active support from senior management. Decisions and actions that are part of the system life cycle include:

- Improving security program,

- Improving security program procedures,

- Improving or refining security controls,

- Integrating security within existing and evolving IT architecture, and

- Improving mission processes and risk management activities.

Each of these decisions results from a continuous improvement and refinement program instilled within the organization. At Level 5, the understanding of mission-related risks and the associated costs of reducing these risks are considered with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures.

2.8 - Findings and Weaknesses

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Weaknesses form the basis for CISS Action Plans (see section 2.9 of this appendix for a description of Action Plans). Findings and non-compliant CSRs form the basis of Weaknesses.

Every Finding and every non-compliant CSR must be addressed by a Weakness record in the CISS. A Finding is any deficiency identified and reported during an audit or review—whether internal or external. For example:

> "Login accounts exist for employees who have left the company."

A Weakness, in this context, would be the underlying cause for, or source of, the Finding (or CSR non-compliance). For example:

> "No policy exists for the removal of accounts when employees leave."

A Weakness must be identified for each Finding. However, a single Weakness may address several Findings and/or non-compliant CSRs. Consider the following simplified illustration:

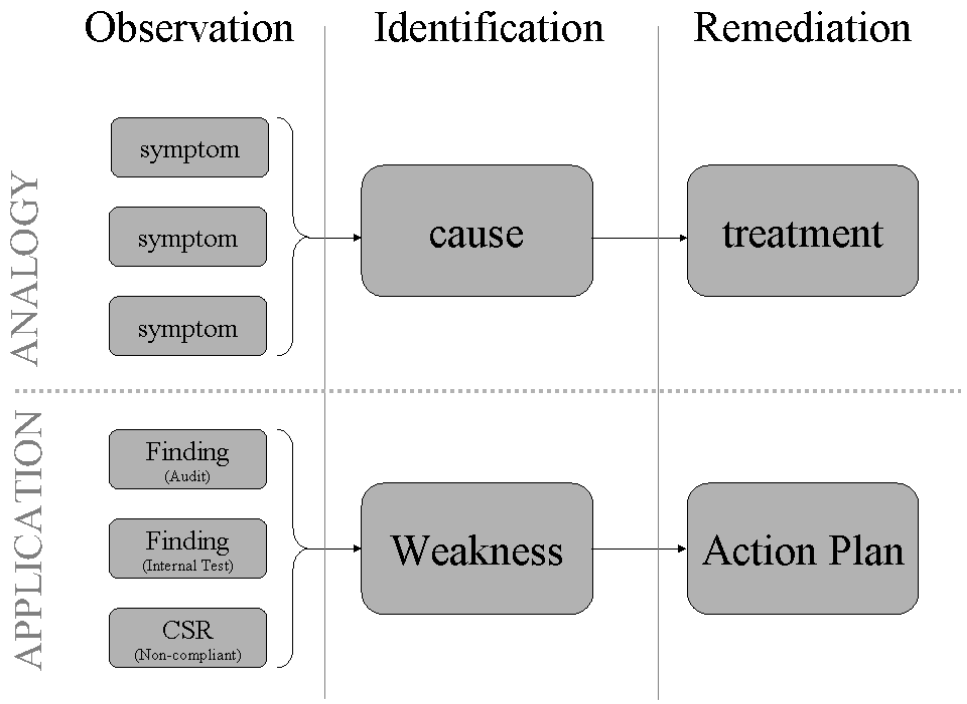

Figure A-2. Analogy for Finding-Weakness-Action Plan Relationship

An Action Plan must be designated to address each Weakness.

Weaknesses that need to be recorded and tracked can be identified either reactively or proactively. Reactive Weakness determination indicates that outside auditors or reviewers identified Findings leading to the Weakness determination. Proactive Weakness determination occurs by conducting regular program and system reviews using Self-Assessments or internal reviews. Sources of security-related Findings and Weaknesses include, but are not limited to:

- Chief Financial Officer (CFO) /Electronic Data Processing (EDP) Audits related to annual CFO Financial Statement Audits (which may include network vulnerability assessment/security testing (NVA/ST)
- Statement on Auditing Standards No. 70 (SAS 70) Audits
- Submission of a Certification Package for Internal Controls (CPIC)
- HHS OIG IT Controls Assessment
- Financial reviews conducted by the General Accounting Office (GAO)
- Annual Compliance Audits (ACAs)
- Section 912 Evaluations or Testing
- Data center system tests
- Penetration/ External Vulnerability Assessment (EVA) tests
- Self-Assessments
- Risk assessments
- Internal or self-directed reviews, audits, or tests.

This list is not exhaustive; there are many avenues for discovering Weaknesses. Because the CISS is used to conduct Self-Assessments as well as a repository for IT audit findings, a distinction is made between Weaknesses that are initiated due to non-compliant CSRs during a Self-Assessment and those initiated from any other type of audit or review. In the CISS, any Weakness that does not result from a self-assessment non-compliant CSR is considered to have resulted from some type of audit or review This distinction becomes important when following the flow in Figure A-3, which shows how security-related Weaknesses are linked and reported.

The CMS business rules (and the CISS tool) require that all Weaknesses be associated with at least one non-compliant CSR response. It is expected that a Weakness will often be associated with both audit Finding(s) and at least one non-compliant CSR(s). In such cases, the flow in Figure A-3 must be followed through both paths after the first decision to ensure that the Weakness is linked to all applicable CSRs and Findings.

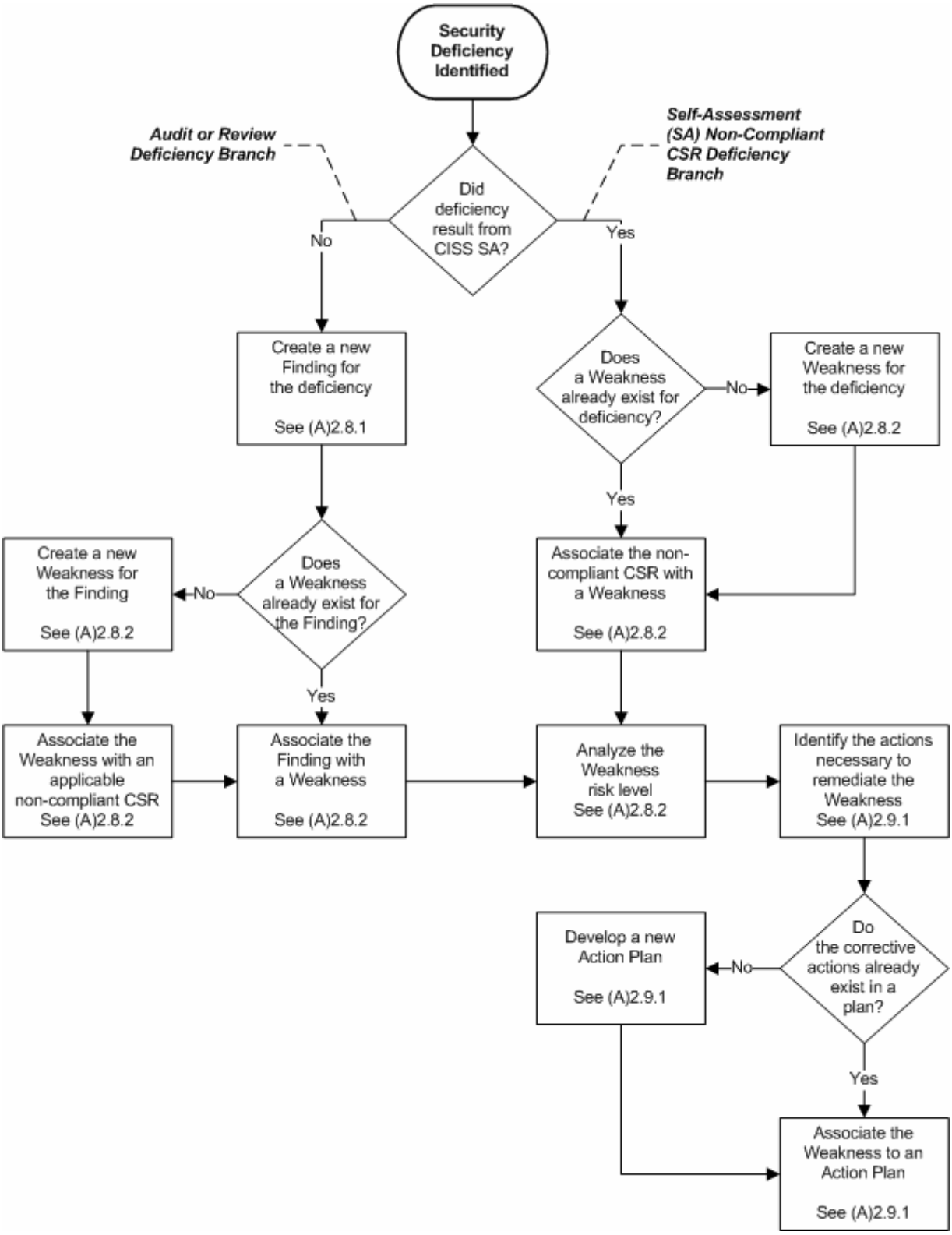

Figure A-3. Weakness Decision Tree

2.8.1 - Findings
(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

All security-related Findings identified or reported by internal or external audits and reviews must be entered into the CISS and associated with (i.e., linked to) one Weakness. At least one non-compliant CSR (i.e., having a response status other than “Level 3,” “Level 4,” “Level 5,” or “N/A”) must also be associated with (i.e., linked to) a Weakness. (ALL Weaknesses MUST be associated with AT LEAST ONE non-compliant CSR, and in addition, MAY also be associated with one or more Findings. Refer to section 2.8.2, Weaknesses)

The following subsections provide guidance for populating the CISS Findings form. Consult the CISS User Guide for specific instructions related to accessing and working with CISS Findings form components.

2.8.1.1 - Finding Identifier
(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The Finding identifier is normally the same identifier provided in the audit or review report. If an internal Finding is identified, the Finding is recorded by a unique identifier consisting of the following information:

a. **Entity**. The first three or four characters are letters that identify the name of the Business Partner. These Business Partner-identifying letters are listed under contractor abbreviations in Chapter 7, Internal Control Requirements, section 40.3, CMS Finding Numbers, of the Medicare Financial Manual (CMS Pub 100-6).

NOTE: This unique Business Partner identifier is not reported to agencies outside of CMS nor is it included in CMS' annual or quarterly POA&M submissions to the OMB. Findings reported outside CMS cannot be traced to a Business Partner.

b. **Year**. The next digits denote the Fiscal Year (FY) in which the Finding was identified and first reported. The year is normally the same as assigned in the audit or review report.

c. **Code**. The next one or two characters identifies the type of review or audit. They are as follows:

- R - Accounts Receivable review
- C - CPIC, (your annual self certification package)
- E - CFO EDP review
- F - CFO Financial review
- S - Statement on Auditing Standards no. 70 (SAS 70)

- O - OIG reviews (HHS Office of Inspector General [Information Technology] controls assessment)
- G - GAO reviews (financial reviews)
- P - CMS 1522 workgroups reviews
- V - CFO related NVA/ST
- N - SAS 70 Novation;
- M - CMS CPIC workgroup reviews
- 9T - Section 912 Testing
- 9E - Section 912 Evaluations
- AC - CMS self-assessment Annual Compliance Audits
- IR - Internal reviews initiated by the entity to meet other Federal requirements, and
- RA - Issues identified during routine risk assessments.

d. Num. The next three digits are the sequential Finding number assigned to each individual Finding beginning with 001, 002, 003, etc. The number is normally the same as assigned in the audit or review report.

2.8.1.2 - Finding Title and Description

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The Finding title should not include any Business Partner-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the Business Partner reporting the Finding, or the location, facility, system, or application to which the Finding refers. Some appropriate Finding titles might include: "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not performed prior to system access," "insufficient physical access controls," etc.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information, such as: "Telnet port open, allowing access by outside users." The title should also be unique enough to be more readily identifiable by name than by number. The Finding title reported in the audit or review report should generally be used, unless that title is too long or contains sensitive descriptive information.

The Finding description should be the descriptive Finding information reported in the audit or review report. This description is not reported beyond CMS, so there is no restriction on its content. If the Finding is the result of an internal audit or review, the description should include

the Finding information required by the GAO, “Government Auditing Standards,” GAO-03-673G (http://www.gao.gov/govaud/yb2003.pdf), commonly referred to as the “Yellow Book.”

2.8.1.3 - Finding Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

All security-related Findings must include a status that indicates the stage or state of the Finding corrective action. Since a Weakness may be associated with multiple Findings, one or more Findings associated with the Weakness can be closed while the Weakness remains open. The four Finding status reporting choices are:

- **On-going**. The Finding remains open and action is on-going to correct it. However, if the Initial Target Completion Date entered in the Action Plan has passed and action is still on-going to correct the Weakness, the status must be reported as Delayed.

- **Closed Pending**. (1) If the Finding was discovered in an internal review, the Business Partner should proceed directly to the Closed status. (2) If the Finding was reported by a CMS-initiated audit or review, the Business Partner should use this status when it considers the Finding closed. However, CMS requires this type of Finding closure to be validated before it is considered Closed. The Business Partner should continue to report the status as Closed Pending until the closure is validated and CMS provides documentation confirming the Closed status. The CISS will require that appropriate documentation be attached to this status to confirm the closure. This documentation should address all aspects of the stated Finding and be sufficient for CMS validation of closure.

- **Closed**. If a Finding has been officially closed by the CMS Office of Financial Management (OFM) in a letter submitted to the Business Partner, it should be reported as Closed in the CISS. The CISS will require that appropriate missing or updated documentation not previously sent be attached to this Closed status to confirm the closure. This documentation must also include any CMS closure letters.
- **Delayed**. Action is on-going to correct the Finding but the Initial Target Completion Date entered in the Action Plan has passed. The Finding should continue to be reported as Delayed until the Finding is corrected and reported as closed.

2.8.1.4 - Determination of Finding Risk Level

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Federal Information Security Management Act (FISMA) of 2002 guidance requires that all Weaknesses be prioritized to ensure that significant IT security Weaknesses take precedence and are immediately mitigated. Since a Finding indicates a Weakness, a risk level must also be assigned to each Finding.

System Finding risk levels should be determined in the system's risk assessment. The risk level determination process is the same for both Findings and Weaknesses and is summarized in section 2.8.2.9, Determining Risk.

2.8.1.5 - Finding FMFIA and CPIC Severity
(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Findings, and their associated Weaknesses, should be disclosed as Material Weaknesses or Reportable Conditions if they have an impact on the Business Partner's internal control structure. Every Finding identified as an internal control deficiency should be categorized as either a Material Weakness or a Reportable Condition based on the following definitions:

- A **Reportable Condition** exists when the internal controls are adequate in design and operation and reasonable assurance can be provided that the intent of the control objective is met, but deficiencies were found during the review that require correction.
- A **Material Weakness** exists when the Business Partner fails to meet a control objective. This may be due to a significant deficiency in the design and/or operation of internal control policies and procedures. Because of these shortfalls in internal controls, the Business Partner cannot provide reasonable assurance that the intent of the control objective is being met.

2.8.1.6 - Finding Category
(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

All Findings must be assigned to one of the following categories. These categories are available from a drop-down menu in the CISS.

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorized Processing (C&A)
- Systems Security Plan
- Personnel Security
- Physical Security
- Production I/O Controls
- Contingency Planning
- H/W and Systems Maintenance
- Data Integrity
- Documentation

- Security Awareness, Training, and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

2.8.1.7 - Finding Point(s) of Contact

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

For each Finding reported, a primary POC must be selected. While multiple POCs can be assigned to a Finding, only one POC can be designated as primary for each Finding. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Finding. Non-primary POCs can include anyone who will assist the primary POC in resolving the Finding.

2.8.2 - Weaknesses

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All security-related Weaknesses identified by internal or external audits and reviews, including Self-Assessments, must be entered into the CISS and associated with (i.e., linked to) an Action Plan *AND* one or more Findings. *The* Weakness must also be associated with a non-compliant CSR and its response status changed accordingly since the Weakness represents a non-compliant CMS security requirement.

Weaknesses resulting from Self-Assessment non-compliant CSRs (i.e., a response status other than “Level 3,” “Level 4,” “Level 5,” or “N/A”) may also be associated with (i.e., linked to) existing Findings but normally are not associated with Findings. Weaknesses derived from a non-compliant CSR do not require an association to a Finding. However, ALL Weaknesses MUST be associated with AT LEAST ONE non-compliant CSR.
The following subsections provide guidance for populating the CISS Weakness form. Consult the CISS User Guide for specific instructions related to accessing and working with CISS Weakness form components.

2.8.2.1 - Weakness Identifier

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Each Weakness must be identified and recorded by a unique identifier consisting of the following information:

a) **Entity**. The first three or four characters are letters that identify the name of the Business Partner. These Business Partner identifying letters are listed under contractor abbreviations in Chapter 7, Internal Control Requirements, section 40.3, CMS Finding Numbers, of the Medicare Financial Manual.

NOTE: This unique Business Partner identifier is not reported or included in CMS' annual or quarterly POA&M submissions. Therefore, Weaknesses reported outside CMS cannot be traced to a Business Partner by any information included in the Weakness identifier.

b) **Quarter**. The next single character represents the FY quarter in which the Weakness was first identified and entered into the POA&M, where:

A = 1st Quarter
B = 2nd Quarter
C = 3rd Quarter
D = 4th Quarter

c) **Year**. The next digits are the FY in which the Weakness was identified and first reported.

d) **Number**. The next number is incremental, representing the sequence in which the Weakness was entered into the Business Partner's POA&M.

For example, a Weakness identified as "CMS_B_2005_3" indicates this CMS Weakness was identified and first reported during the 2nd quarter of FY 2005, and it is the 3rd Weakness identified during that time period.

2.8.2.2 - Weakness Title and Description

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The Weakness title should not include any Business Partner-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the Business Partner reporting the Weakness, which location or facility has the Weakness, or what system or application has the Weakness.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information. The title should also be unique enough to be more readily identifiable by name than by number.

The Weakness description, however, is not reported beyond CMS, and it should provide sufficient information and detail to allow CMS to evaluate the Weakness.

2.8.2.3 - Weakness Category

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

All Weaknesses must be assigned to one of the following categories. These categories are available from a drop-down menu in the CISS:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorized Processing (C&A)

- System Security Plan
- Personnel Security
- Physical Security
- Production I/O Controls
- Contingency Planning
- H/W and Systems Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training, and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails.

2.8.2.4 - Determination of Weakness Risk Level

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

System Weakness risk levels should be determined in the system's risk assessment according to criteria in the CMS Information Security Risk Assessment (RA) Methodology.

2.8.2.5 - Weakness FISMA Severity

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

FISMA requires the reporting of any significant deficiency in a policy, procedure, or practice to be identified as a material Weakness under the Federal Managers Financial Integrity Act (FMFIA), and if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (FFMIA). Depending on the risk and magnitude of harm that could result, Weaknesses identified during the review of security controls are reported as deficiencies in accordance with OMB Circular No. A 123, “Management Accountability and Control,” and FMFIA.

Although the CISS includes the three FISMA Severity levels listed below, only one level is activated and available for use by Business Partners (i.e., Weakness). The other two severity levels, Significant Deficiency and Reportable Condition, require that CMS make a risk-based decision before a Weakness can be assigned to them. Should CMS make that determination, additional guidance will be provided on how to select a different severity level.

The three FISMA Severity levels are:

- **Weakness.** The term Weakness refers to any and all other IT security Weaknesses pertaining to the system.

  NOTE: This is the only severity level that can be selected by Business Partners at this time.

- **Reportable Condition.** A Reportable Condition exists when a security or management control Weakness does not rise to a significant level of deficiency*;* yet*, it* is still important enough to be reported to internal management. A security Weakness *may* be considered a Reportable Condition *even though it is* not deemed to be a Significant Deficiency by agency management *if it* affects the efficiency and effectiveness of agency operations. However, due to lower risk, corrective action may be scheduled over a longer period of time.

- **Significant Deficiency**. *A Significant Deficiency exists* when a Weakness in an agency's (i.e., CMS) overall information systems security program or management control structure, or within one or more information systems, significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

2.8.2.6 - Weakness Type

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

There are two types of security-related Weakness that must be identified:

- **Program Weakness**. A Program Weakness impacts multiple IT systems as a result of a deficiency in the IT security program.

- **System Weakness**. A System Weakness pertains to the management, operation, or technical controls of a specific IT system.

2.8.2.7 - Weakness Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

All security-related Weakness corrective actions must include a status that indicates the stage or state of the Weakness corrective action. Since multiple Findings may be associated with a Weakness, the Weakness cannot be closed until all Findings associated with it are closed. The five Weakness status reporting choices are:

- **On-going**. The Weakness remains open and action is on-going to correct it. However, if the Initial Target Completion Date entered in the Action Plan has passed and action is still on-going to correct the Weakness, the status must be reported as Delayed.

- **Closed Pending**. (1) If the Weakness was discovered in an internal review or Self-Assessment, the Business Partner should proceed directly to the Closed status. (2) If the Weakness resulted from a CMS-initiated audit or review, the Business Partner should use this status when it considers the Weakness closed. However, CMS requires this type of Weakness closure to be validated before it is considered Closed. The CISS will require that appropriate documentation be attached to this status to confirm the closure. This documentation should address all aspects of the stated Weakness and be sufficient for CMS validation of closure.

- **Closed**. If a Weakness has been officially closed by the CMS Office of Financial Management (OFM) in a letter submitted to the Business Partner, it should be reported as Closed in the CISS. The CISS will require that appropriate missing or updated documentation not previously sent be attached to this Closed status to confirm the closure. This documentation must also include any CMS closure letters.

- **Delayed**. Action is on-going to correct the Weakness but the Initial Target Completion Date entered in the Action Plan has passed. The Weakness should continue to be reported as Delayed until the Weakness is corrected and reported as closed.

2.8.2.8 - Weakness Point(s) of Contact

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

For each Weakness identified, a primary POC must be selected. While multiple POCs can be assigned to a Weakness, only one POC can be designated as primary for each Weakness. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Weakness. Non-primary POCs can include anyone who will assist the primary POC in resolving the Weakness.

2.8.2.9 - Determining Risk

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The risk determination process explained in this section is taken from the CMS Information Security *(IS)* Risk Assessment (RA) Methodology. The process described here assumes that specific threats and vulnerabilities have already been identified. Consult the CMS *IS* RA Methodology for specifics on identifying threats and vulnerabilities.

While both system and business risk measurements are discussed and combined in the CMS *IS* RA Methodology document, risk determinations made in and by the CISS are for systems only. *The goal of risk determination is to calculate the level of risk for each threat/vulnerability pair based on:*

1. *The likelihood of a threat exploiting a vulnerability; and*

2. *The severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of CIA.*

2.8.2.9.1 - *Likelihood of Occurrence*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The risk likelihood level is determined by considering known threats as they may apply to known system vulnerabilities. *The likelihood is an estimate of the frequency or the probably of such an event. The likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access, and existing controls; the presence, motivation, tenacity, strength, and nature of the threat; the presence of vulnerabilities; and the effectiveness of existing controls.*

Refer to the information in Table A-4 for guidelines to determine the likelihood of occurrence that a threat is realized and exploits the system's vulnerability.

Table A-4. Likelihood of Occurrence Levels

Likelihood	Description
Negligible	*Unlikely to occur.*
Very Low	*Likely to occur two/three times every five years.*
Low	*Likely to occur once every year or less.*
Medium	*Likely to occur once every six months or less.*
High	*Likely to occur once per month or less.*
Very High	*Likely to occur multiple times per month.*
Extreme	*Likely to occur multiple times per day.*

2.8.2.9.2 - *Impact Severity*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The severity of impact is the magnitude or severity of impact on the system's operational capabilities and data if the threat is realized and exploits the associated vulnerability. The severity of impact for each threat/vulnerability pair is determined by evaluating the potential loss in each security category (CIA) based on the system's information security level as explained in BPSSM Section 4.0, Information and Information Systems Security Categorization. The impact can be measured by loss of system functionality, degradation of system response time, or inability to meet a CMS business function, dollar losses, loss of public confidence, or unauthorized disclosure of data.

Refer to Table A-5 for guidelines to determine system impact severity levels.

Table A-5. System Impact Severity Levels

Impact Severity	Description
Insignificant	*Will have almost no impact if threat is realized and exploits vulnerability.*
Minor	*Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.*

Significant	*Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.*
Damaging	*May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.*
Serious	*May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of Government information or services.*
Critical	*May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.*

2.8.2.9.3 - *Level of Risk*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The overall risk level can be expressed in terms of the likelihood of the threat exploiting the system vulnerability and the impact severity of that exploitation on the CIA of the system. This overall level of risk is depicted in the following equation:

Level of Risk = Likelihood of Occurrence x Impact Severity

After the risk likelihood *of occurrence* and impact *severity* have been established, the overall *level of* risk is determined using the following risk level matrix (Table A-6). The level of risk equals the intersection of the likelihood *of occurrence* and impact *severity* values. The CISS determines this value automatically based on the input values of the Weakness likelihood *of occurrence* and impact *severity selections*.

Table A-6. Overall Risk Level Matrix

Likelihood of Occurrence	Impact Severity					
	Insignificant	**Minor**	**Significant**	**Damaging**	**Serious**	**Critical**
Negligible	*Low*	*Low*	*Low*	*Low*	*Low*	*Low*
Very Low	*Low*	*Low*	*Low*	*Low*	*Moderate*	*Moderate*
Low	*Low*	*Low*	*Moderate*	*Moderate*	*High*	*High*
Medium	*Low*	*Low*	*Moderate*	*High*	*High*	*High*
High	*Low*	*Moderate*	*High*	*High*	*High*	*High*
Very High	*Low*	*Moderate*	*High*	*High*	*High*	*High*
Extreme	*Low*	*Moderate*	*High*	*High*	*High*	*High*

2.9 - Action Plans and POA&Ms

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Action Plans form the basis for the periodic POA&M reporting requirement (see section 3.5.2 of the BPSSM for reporting requirements).

The CISS assists Business Partners in reporting Weaknesses, preparing Action Plans, and submitting the required POA&Ms to CMS. The POA&M submission process is automatic, in that it contains information already entered into the CISS. Therefore, no further guidance is required beyond the instructions found in section 11, Submissions to CMS, of the CISS User Guide. The remainder of this section is devoted to guidance for populating the CISS Action Plan form.

2.9.1 - Completing Action Plans

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

Each Weakness entered into the CISS must correspond to an Action Plan for its resolution. Although the CISS does permit multiple Weaknesses to be addressed by a single Action Plan, this approach is not recommended, because a Weakness cannot be closed until its corresponding Action Plan has been completed.

Corrective action methods should be analyzed for appropriateness in fully resolving any associated Weakness; they should also be viewed for long-term implications. When completing an Action Plan, the cost for each option must be estimated and analyzed to determine short- and long-term solution capabilities.

2.9.1.1 - Action Plan Title and Description

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The Action Plan title should not include any Business Partner-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the Business Partner reporting the Weakness, which location or facility has the Weakness, or what system or application has the Weakness. The title is used only to provide a descriptive name to the Action Plan so it can be distinguished from other Action Plans.

Detailed descriptions of Action Plans are necessary, and sufficient text is required to permit oversight and tracking. Sensitive information should not be revealed in the description of the Action Plan, Weakness, or associated Milestones. In addition, no Business Partner-, location-, or system-specific information should be included in the Action Plan description. Otherwise, the descriptive information can be used to identify the Business Partner, location or facility, or system or application.

2.9.1.2 - Determining Completion Dates

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The Completion Dates (i.e., Initial Target, Current Projected, and Actual) are populated automatically based on dates entered in the Milestones. These dates will change based on the Milestone dates until the Action Plan is reported in a POA&M submission. Once the Action Plan has been initially submitted to CMS, the Initial Target date is locked and cannot be changed. So, when completing Milestones, completion dates should be determined based on realistic timelines for resources to be obtained and associated steps to be completed. For example, although it may take 30 days to complete the required Action Plans for a specific Weakness, it may not be possible to complete ALL Action Plans for all Weaknesses during the same time period due to staffing resource limitations. Therefore, the Initial Target Milestone dates should be based on the outcome of prioritization decisions and resource availability.

2.9.1.3 - Determining Costs

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

In determining Weakness remediation costs, Business Partners must consider the following criteria to determine security costs for a specific IT investment:

a) The products, procedures, and personnel (Business Partner employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. This includes the costs of:

- Risk assessment
- Security planning and policy
- Certification and accreditation
- Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
- Authentication or cryptographic applications
- Education, awareness, and training
- System reviews/evaluations (including security control testing and evaluation)
- Oversight or compliance inspections
- Development and maintenance of Business Partner reports to CMS and corrective Action Plans as they pertain to the specific investment
- Contingency planning and testing
- Physical and environmental controls for hardware and software
- Auditing and monitoring
- Computer security investigations and forensics

- Reviews, inspections, audits, and other evaluations performed on Business Partner facilities and operations.

b.) Security costs must also include the products, procedures, and personnel (Business Partner employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; system administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.

c.) Many Business Partner corporate entities operate networks that provide some or all of the necessary security controls for the associated applications. In such cases, the Business Partner must nevertheless account for security costs for each application investment. To avoid "double-counting," Business Partners should appropriately allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, Business Partners may find it helpful to ask the following simple question: "If there were no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" If Business Partners encounter difficulties with the above criteria, they must contact CMS prior to submission of their POA&M report.

Target Implementation Costs are the total costs for implementing the remediation safeguards during the first year of implementation. This will include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. Since this cost may be used for budgetary purposes, it must be as accurate as feasible. It is advised that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted when estimating this cost.

The Estimated Annual Maintenance cost is the projected recurring cost of implementing the remediation safeguards. This is the projected recurring cost to CMS to maintain this remediation safeguard for the following FY. This cost must include depreciation, amortization, etc. Costs associated with continued funding should be added to subsequent line one charges where applicable.

The Percent Security value is the percentage of the total remediation safeguard costs that pertain or apply to security.

The Percent Applied to CMS is the percentage of the total remediation safeguard cost being charged to CMS. This is the percentage of cost that CMS will fund for safeguards that will be shared between CMS (Medicare) systems and corporate systems.

2.9.1.4 - Determining Funding Sources

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The CISS requires that some resources be identified for every Action plan. Action Plans cannot be executed without the application of resources (personnel or procurement). Therefore, the CISS will not accept "zero-cost" Action Plans. Resources for Weakness remediation can be obtained through the following means:

- Using current resources marked for security management of the system or program. This will be the method used for resourcing most Weaknesses.
- Reallocating existing funds or personnel.
- Requesting additional funding.

Requesting new or additional funding from CMS to remediate a Weakness should only be used when no other source of funding can be identified. When funding is available, CMS will prioritize funding allocations based on Weakness prioritization and risk levels. It is in the Business Partner's best interest to use current resources or reallocate existing funds or personnel to remediate all Weaknesses. All funding reallocations must be approved by CMS.

2.9.1.5 - Milestone Title and Description

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

The Milestone title should not include any sensitive or identifying information. The title should be descriptive enough to distinguish one Milestone from another.

Detailed descriptions of Milestones are not necessary, but sufficient data is required to permit oversight and tracking. Sensitive or identifying information should not be revealed in the Milestone descriptions.

2.9.1.6 - Milestones with Completion Dates

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Fundamentally, the Action Plan is simply a container for the Milestones that will address remediation of any corresponding Weakness. The Milestones are identified in the POA&M, and each one should correspond to a specific corrective action. Ideally, there should be at least one Milestone per quarter so that Action Plan progress can be tracked in the POA&M submissions to CMS.

Including anticipated completion dates with each Milestone enables progress toward Weakness mitigation to be tracked. Each Milestone within the POA&M should include an anticipated date of completion (Projected Date). Once Milestones and completion dates are entered, changes can be made until the Action Plan is first submitted.

The overall projected complet*ion* date of the Action Plan is derived automatically by the CISS based on the projected completion dates of all of the Milestones. The Initial Target date remains unchanged on*c*e the Action plan has been submitted to CMS. However, the Current Projected

Date will adjust automatically based on changes in milestone projected completion date. (Note that the Action Plan status of “Delayed” is always calculated based on the Initial Target date.)

Milestones should effectively communicate the major steps within an Action Plan that will be performed to mitigate a Weakness. For example, appropriate Milestones for an Action Plan associated with a Weakness such as “Identification and authentication process need to be more stringent” might read:

- Evaluate methods for strengthening identification and authentication
- Develop procedures to standardize accepted authentication process
- Acquire management approval/sign-off of new process and procedures
- Implement approved authentication process

2.9.1.7 - Milestone Changes

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

If a situation exists that prevents a Milestone and/or overall corrective action from being completed on time, the new estimated date of completion will automatically be reflected in the Current Projected date based on the Milestone changes. However, once the Action Plan has been submitted, the Initial Target date field is locked and cannot be changed. Any changes to a Milestone should include the reason(s) for the delay.

Appendix B

Medicare Information Technology (IT)
Systems Contingency Planning

Table of Contents

(Rev. 8, 04-06-07)

1.0 - Introduction

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

CMS business partners are required by CMS CSR 5.2 to develop and maintain a contingency plan. This plan is to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption.

Section 3.4 of this document requires that all CMS Medicare business partners prepare, review, and test their Medicare IT systems contingency plans. All General Support Systems (GSS) and Major Applications (MA) that support critical Medicare operations must be covered by a Medicare IT Systems Contingency Plan (CP).

This document presents the direction for accomplishing Medicare IT systems contingency planning. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an IT systems contingency plan, or updating an existing plan.

The business partner information security risk assessment may be used as a checkpoint to determine if appropriate contingencies have been addressed in the contingency plan.

To ensure the contingency plan is workable, it must be thoroughly and periodically tested.

The simplified diagram in Figure B-1 illustrates the IT systems contingency planning process.

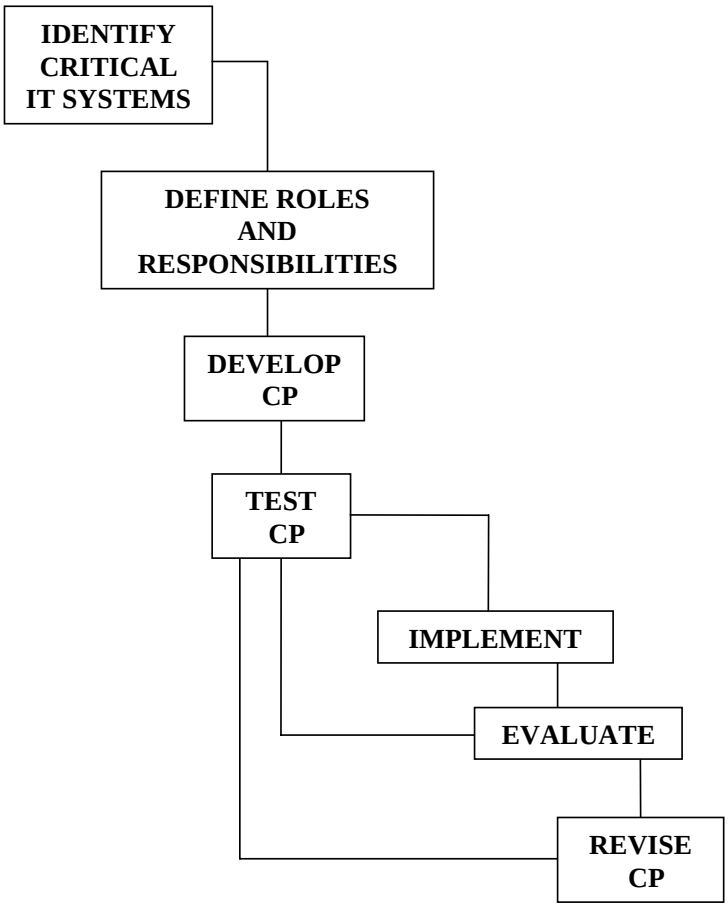

Figure B-1 – IT Systems Contingency Planning Process

2.0 - Scope

(Rev. 3, 03-28-03)

The business partner IT systems contingency plans address organizations and sites where Medicare data is processed, including claims processing locations, data centers, and other processing or printing sites.

3.0 - Definition of an Acceptable Contingency Plan

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A contingency plan is a document that describes how to plan for and deal with an emergency or system disruption. These situations could be caused by a power outage, hardware failure, fire, or terrorist activity. A contingency plan is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.

Protecting lives is the paramount task while executing a contingency plan.

Before developing an IT systems contingency plan, it is advisable to have or create a contingency policy. The contingency plan must be driven by a contingency policy. The

contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

The IT systems contingency plan should be developed under the guidance of IT management and systems security persons and all organizational components must be actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.

It can be a very subjective argument relative to what constitutes an acceptable contingency plan. In this document, the description of an acceptable contingency plan is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner contingency plans and test reports.

The following summary statements define what constitutes an acceptable contingency plan. This is not an all-inclusive list and the topics are not in any order of importance or priority.

1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.

2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.

3. Considers risk assessment results.

4. Addresses possible and probable emergencies or system disruptions.

5. Can be sufficiently tested on an established regular basis at reasonable cost.

6. Contains information that is needed and useful during an emergency or system disruption.

7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.

8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.

9. Clearly defines the resources necessary to implement the plan.

10. Reflects what can be done – is not a wish list.

11. Assumes people will use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe pressure.

12. Addresses backup and alternate sites.

13. Addresses the use of manual operations, where appropriate and necessary.

14. Contains definitive “Call Lists” to use for contacting the appropriate persons in the proper sequence. This list would include vendor points of contact.

An acceptable contingency plan should be straight to the point. It should not contain any more information than is necessary to plan for and implement contingency actions. The users should not get bogged down in detail as they read the plan to determine what to do, when to do it, what is needed to do it, and who should do it. The contingency plan should serve as a “user’s manual” and be easy to understand and use.

Because a contingency plan is designed to be used in a stressful situation, *i*t must be written with that as a foremost thought in mind. The prime objective is to maximize the continuity of critical operations.

Reviewing a contingency plan and testing it will help determine whether it remains an acceptable plan. The review and testing should not focus solely on content, but must also focus on ease of use.

A complete set of contingency plans for an organization may be made up of several smaller contingency plans, one for each business function (e.g. claims processing) or for a single data center, for example. This breakdown into manageable parts helps to keep a plan easy to use.

Careful thought should be given to the organization of the contingency plan. The organization should be logical in terms of what will the user want to know or do first. If the first thing that should happen in an emergency is that a call list should be used to notify persons, then that call list, or a pointer to it, should be placed very near the front of the contingency plan. Not every informational item to be utilized during a contingency event will be in the contingency plan document. *For example,* the plan may point to an attachment or to a separate procedures manual. In this regard, a contingency plan should contain a very understandable and useful table of contents, so that a user can quickly find the information being sought.

Contingency planning can provide a cost-effective way to ensure that critical IT capabilities can be recovered quickly after an emergency. IT systems contingency planning should embrace a coordinated contingency policy of what will be done to fully recover and reconstitute all operations.

4.0 - Medicare IT Systems Contingency Planning
(Rev. 3, 03-28-03)

The goal of IT systems contingency planning is to continue accomplishing critical Medicare IT systems operations in an emergency or system disruption and to accomplish a rapid and smooth recovery process.

4.1 - Contingency Planning
(Rev. 3, 03-28-03)

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process must address all the actions and resources needed to ensure continuity of operation of critical Medicare IT systems and the means of implementing the needed resources. IT management and staff must be trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located. Contingency planning includes such training.

It is advisable to establish a Medicare IT systems contingency planning team. This team would be responsible for defining critical Medicare IT systems, including applications software, data, processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 - Coordination With Other Business Partners

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning must include those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links must be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5.0 - Medicare IT Systems Contingency Plan

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The following format may be used in developing an IT system contingency plan. While this format is not required, all of its elements must be included in the Contingency Plan.

1. Introduction
    - Background
    - Purpose/Objective
    - Management commitment statement
    - Scope
        - Organizations
        - Systems
        - Boundaries

- IT capabilities and resources
- CP policy
    - Priorities
    - Continuous operation
    - Recovery after short interruption
    - Minimum recovery times

2. Assumptions
3. Authority/References
4. Definition of what the CP addresses
    - Organizations
    - Systems
    - Boundaries
5. Three phases defined
    - Respond
    - Recover
    - Restore/reconstitute
6. Roles/Responsibilities defined
7. Definition of critical functions
8. Alternate capabilities and backup
9. Definition of required resources to respond and recover
10. Training
    - CP must address Who – When – How
11. Testing the CP
    - Philosophy
    - Plans
    - Boundaries
    - Live vs. Walkthrough
    - Reports
    - Responsibilities
12. CP maintenance/updating

Schedule

13. Relationships/Interfaces
    - Outside (vendors, providers, banks, utilities, services, CMS)
    - Internal
    - Dependencies
14. Attachments
    - Actions for each phase
    - Procedures
    - Call trees
    - Vendor contact list
    - Hardware inventory
    - Software inventory
    - System descriptions
    - Alternate/Backup site information
    - Assets/Resources
    - Risk Assessment Summary (refer to System Security Plans)
    - Agreements/Memos of Understanding
    - Manual Operations
    - Supplies/Materials/Equipment
    - Floor plans
    - Maps

The contingency plan must provide for off-site storage of:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the contingency plan
- Administrative supplies (forms, blank check stock, etc.).

6.0 - Testing
(Rev. 3, 03-28-03)

The CMS requires testing of the contingency plan annually under conditions that simulate an emergency or a disaster. (CSR Category 5.)

The CMS requires that the critical IT systems must be tested annually and the contingency plan updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 - Claims Processing Data Centers
(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

Many of the contractors with which CMS has direct contracts do not have their own data centers. They usually contract this service out. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they must have a contingency plan.

6.2 - Multiple Contractors
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Data centers usually serve multiple contractors. Existing shared processing environments allow for multiple contractors to process claims at a data center. There are numerous data centers processing Part A and Part B claims for multiple Medicare contractors.

It is important to test a contingency plan at a data center that serves multiple contractors. This provides a mechanism to examine the possible commingling of data between contractors, wherein data may be compromised.

Before testing of the contingency plan begins, it is important to understand how contractor data is protected and/or kept separate. The data centers may use a security package, such as ACF, to control access and separation of data. In order to perform appropriate testing, the complexity of the data center operation must be understood.

6.3 - Test Types
(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Contingency plan test guidance suggests three types of testing:

- Walkthrough
- Simulation/modeling
- Live

These are defined below:

- **Walkthrough**: A walkthrough test is accomplished by going through a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented *so* that they can be logically followed. A "test team" might sit around a table and talk through each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but *they* would not actually start all hardware, software, and communication operations in order to assume the function of the primary site.

- **Simulation/Modeling**: Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster or the number of people that can get to an alternate site following a disaster.

  Simulation involves taking physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team *does* the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

- **Live**: This is the most complete and expensive test to accomplish. It involves *completing the physical steps that would actually be taken* if an emergency occurred. People and materials would be moved to an alternate site for the test*, and s*ervers would actually be shut down to reduce capability. Power would be shut off*, and l*ive conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications*,* and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end). When conducting end-to-end testing, items to consider include:

- End-to-end testing can be *completed* as part of walkthrough or live test.

- Not testing end-to-end means that some links, processes, or subsystems are missed.

- What is the risk in not *conducting* end-to-end testing?

- Live end-to-end testing can be very expensive!

Considering risks and cost, management must make a decision as to what type and scope of testing is appropriate.

6.3.1 - Live vs. Walkthrough

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

- High-level testing can take the form of a walkthrough test.
- A walkthrough can be part of the overall testing process, but not the whole process.
- Lower-level testing can include a walkthrough, if live testing is not an option.
    - Live testing should be the first choice.
    - Fall back to a simulation/model if live testing is not an option.
    - Cost, time, and interruption of normal operations are major considerations in doing a live test.
    - A walkthrough test should be the last resort.
        - Ask what a walkthrough test would miss.
        - Consider the ramifications of missing that part of the test.
        - Remember that there is risk in not doing a live test—can the risk be accepted?
    - Consider the criticality of functions, processes, and systems.
    - If critical to continuing essential business operations, then these are strong candidates for live testing.
- Testing interfaces.

  It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a "walkthrough" method. Simulation or "live" testing is preferred.
- Cost and complexity.

  The decision as to how to test critical functions, processes, and systems must result from careful consideration of complexity and cost. A complete "live" test of all elements of an operation may prove to be extremely costly, in terms of both dollars and time. If that cost out weighs the "cost" of the risk of not doing live testing, then "live" testing should probably be ruled out.

6.3.2 - End-to-End

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This kind of testing aims to ensure that all software and hardware components associated with a function, process, or system are tested from the front end through to the back end (input through process through output). As with live testing, end-to-end testing can be expensive.

- End-to-end testing must only be considered for critical functions, processes, or systems.
- Why is end-to-end testing needed?
- It provides the best assurance that there are no problems.
- Would a partial test be meaningful?
- If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.
- Examples of types of end-to-end tests:
    - Claims receipt through to check generation
    - Query of a database through to the response
    - MSP check request through to check issue and back to MSP.
- Evaluate complexity and cost.

  The decision on how to test critical functions, processes, and systems must carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost out weighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.
- Consider the criticality of functions, processes, and systems.

  Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.
- If you can't do end-to-end testing, then consider live testing of all links possible to help ensure minimum problems.
    - Or, do simulation/modeling.
    - Or, do walkthrough.

Overall testing may take the form of reviews, analyses or simulations of contingencies. Reviews and analyses may be used for non-critical systems, whereas critical systems should be tested under conditions that simulate an emergency or a disaster.

It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems must be tested.

Testing may include activities in addition to computer processing. Manual operations should be checked according to procedures, and changes made as experience indicates.

6.4 - Local Processing Environments (PCs/LANs)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

IT systems contingency plan testing relative to local environments, such as individual or clustered workstations and LAN configurations, may be less comprehensive than data center testing. Reviews and analyses may be used to accomplish certain non-critical systems testing, whereas critical systems require full simulation or live testing. The criticality of the system is the deciding factor relative to what type testing is used, how often tests are accomplished, and how thorough the testing should be.

The decision of which test approach to use relative to a specific system or configuration must be a management decision based on advice from the SSO, IT systems staff, operations and support representatives, and the lead test planner/manager.

6.5 - Test Planning

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

An IT systems contingency test plan must address at least the following:

Test objectives
Required equipment and resources
Necessary personnel
Schedules and locations
Test procedures
Test results
Failed tests
Corrective action management process
Retest
Approvals.

It is advisable to establish test teams responsible for preparing and executing the IT systems contingency plan tests. Responsibilities must be assigned to test team members, including executives, observers, and contractors.

Following testing, the corrections specified in a Corrective Action Management Process must be tested. The process must include:

List of items that failed the previous test
Corrections planned
Retest detail
Schedule
Review responsibilities.

Ensure that the lessons learned from IT systems contingency plan testing are discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation must exist for:

Test plans
Test results
Corrective action management process
Retest plans
Memos of Understanding/Formal Test Arrangements.

7.0 - Minimum Recovery Times

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Recovery time is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity.

Minimum recovery time is the longest acceptable period of time for recovery of operations. If claims processing operations must be recovered within 72 hours, then that is the minimum acceptable time to recover. Anything over that is unacceptable.

- Recovery times will vary, depending on the criticality of the entity involved.
- Times can be from a few minutes to days or weeks.
- A table/matrix can be constructed that lists the recovery times.
- There can be a separate table/matrix for each organization or major function (e.g., claims processing, medical review, check generation).
- Recovery times must be carefully defined and must be achievable.
- *Recovery times* can be verified to some extent through testing (simulation or live).

8.0 - Responsibilities

(Rev. 3, 03-28-03)

Following is a summary of responsibilities for key groups and persons involved with contingency planning.

8.1 - Business Partner Management

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary IT systems contingency planning.

- Ensures that appropriate contingency plans are developed, periodically tested, and maintained.

- Ensures that all IT operations participate in the contingency planning and the development of the plans.

- Reviews the plan and recommendations.

- Requests and/or provides funds for plan development and approved recommendations.

- Assigns teams to accomplish development of test procedures, and for testing the plan.

- Reviews test results.

- Ensures that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.

- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.

- Business partner management must approve:

    - The *C*ontingency *P*lan
    - Changes to the *C*ontingency *P*lan
    - Test Plans
    - Test results
    - Corrective action management processes
    - Retest Plans
    - Memos of Understanding/Formal Arrangement Documents

Changes to storage and backup/alternate site facilities

8.2 - Systems Security Officer (SSO)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Documents the scope and purpose of IT systems contingency planning
Reconciles discrepancies and conflicts
Evaluates security of backup and alternate sites
Leads the preparation of the contingency plan
Submits the plan and recommendations to management
Monitors implementation of the plan and reports status to management
Ensures all testing of the plan is accomplished as required
Reviews test results
Ensures that the plan is updated based on test results.

8.3 - Service Components (provide support functions such as maintenance, physical security)

(Rev. 3, 03-28-03)

- Maintain physical security forces to respond to emergencies.
- Schedule fire and other emergency drills and monitor effectiveness.
- Develop emergency re-supply procedures for forms, supplies, equipment, and furniture.
- Provide for priority replacement of computer hardware.
- Provide for restoring telecommunications.
- Provide for backup sites and procedures.
- Provide information relative to the availability of recovery sites.
- Develop procedures for documenting inventories of equipment and furniture.
- Provide a list of employees' home addresses and phone numbers.
- Support testing of the plan.

8.4 - Operating Components (IT operations personnel)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Designate employees for emergency response teams.
Designate employees for backup teams.
Designate employees for recovery teams.
Provide a list of employees' home addresses and phone numbers.
Identify time-critical operations and systems.
Identify critical resources, such as hardware, software, data, communications, facilities, and people.
Identify supplies (forms, blank check stock, etc.) to be stored at alternate sites.
Identify critical data to be backed up offsite.
Provide information on testing requirements.
Accomplish and/or support end-to-end system testing.
Review test results.
Identify critical non-automated data processing operations.
Review basic service organization plans and advise SSO where needs are not met.
Monitor contingency plan implementation and report status to management.

9.0 - Changes

(Rev. 3, 03-28-03)

The contingency plan must be updated whenever one or more of the following events occurs:

New systems or operations added.
Upgrade or replacement of Standard System software.
Hardware or software replacement.
Changed back up/alternate site.
Changed storage facilities.
Removal of existing systems or operations.

10.0 - Attachments

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Materials that are too extensive to be included in the body of the Medicare IT systems contingency plan must be included as attachments. These should be referenced in the contingency plan. These should also be a part of the Site Security Profile (Refer to CSR Category 1). Existing material that facilitates response, backup, and recovery operations should be included as attachments or a pointer provided. Much of this material is bulky and relates to the entire organization. The SSO must ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the contingency plan. Such material includes:

Master inventories of forms, supplies, and equipment
Description of computer hardware and peripherals
Description of applications software
Appropriate security weakness information
Systems and program documentation
Prioritized schedules for computer operations
Communications requirements, especially computer networks.

11.0 - Checklist

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The following checklist provides a means for determining if a contingency plan contains the appropriate information that can readily be used in handling an emergency or system disruption. This list is not all-inclusive, but rather should serve as a thought stimulus for evaluating contingency plans.

This checklist uses the same outline as the suggested contingency plan format.

1. Introduction
   Does the contingency plan contain:

   - Background
     Is a history of the plan provided? Are the physical environment and the systems discussed?

   - Purpose/Objective
     What does the plan address? Why was it written? What does it aim to accomplish?

- Management Commitment Statement
  Has the contingency plan been approved by management and the SSO? Once the contingency plan is created, reviewed, and ready for distribution, it should be approved by site, operations and information systems management, and the SSO.

- Scope
  Are the boundaries of the plan indicated? What organizations are involved, not involved?
  - Organizations
  - Systems
  - Boundaries

- IT Capabilities and Resources
  Is the focus of the plan on IT systems, capabilities, and resources?

- Contingency Plan Policy

  - Priorities
    - *Are the contingency plan steps ranked according to priority?*

  - Continuous *O*peration
    - Are there functions, processes, or systems that are required to continue without interruption?

  - Recovery after *S*hort *I*nterruption
    - Which functions, processes, or systems can be interrupted for a short time?

  - *Recovery Times?*
    - *Are the recover times stated?*
    - *What are the minimum recovery times?*

  - Standalone Units
    - Does a contingency plan exist for any standalone workstation? A key part of a contingency plan should address any standalone workstations that are part of the critical operations environment. It should state where backup software and support data for these workstations is stored.
    - Is the plan reviewed and approved by other key affected persons?

2. Assumptions
   Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?

3. Authority/References
   - Who or what document is authorizing the creation of the contingency plan?
   - What are the key references that apply to the plan?

4. Definition of what the Contingency Plan Addresses

- Organizations
  To which organizations does the contingency plan apply?

- Systems
  Is there a general description of systems and/or processes?

- Boundaries
  Are the system boundaries clearly defined?

5. Three phases defined
   Does the plan address three phases of emergency or system disruption?

   - Respond
     - Is this phase adequately described so that it is understood what activities occur therein?
     - Is damage/impact assessment considered?
     - Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?

   - Recover
     Is this phase adequately described so that it is understood what activities occur during this phase?

   - Restore/Reconstitute
     Is this phase adequately described so that it is understood what activities occur during this phase?

6. Roles/Responsibilities Defined

   - Has the necessary contingency plan implementation organization been defined and the responsibilities of all those involved clearly stated with no ‘gray areas’?

   - Will all who have a task to perform be aware of what is expected of them?

   - Does the contingency plan assign responsibilities for recovery? The responsibilities of key management and staff persons should be carefully described in the contingency plan, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

   - Does the contingency plan address critical systems and processes?

   - Have emergency processing priorities been established and approved by management?

- Does the contingency plan specify critical data? The contingency plan should specify the critical data needed to continue critical business functions and how frequently the data is backed up.

- Has a list of critical operations, data, and applications been created? In preparation for preparing the contingency plan, a list of current critical operations, data and applications should be prepared and approved by management. *This list should contain the items* needed to continue the critical business functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.

- Does the contingency plan address issues relative to pre-planned alternate locations? The contingency plan must address any potential issues relative to pre-planned alternate locations. These include:
  - insurance
  - equipment replacement
  - phones
  - utilities
  - security

- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities should include:
  - prioritizing operations
  - identifying key personnel and how to reach them
  - listing backup systems and where they are located
  - stocking critical forms, blank check stock, and supplies off-site
  - developing reliable sources for replacing equipment on an emergency basis

- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?

- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?

- Have temporary data storage sites and location of stored backups been identified?

- Is the frequency of file backup documented?

- Have the arrangements been made for ensuring continuing communications capabilities?

- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?

- *Are* system, application, and other key documentation maintained at the off-site location?

- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?

- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.

- Is the contingency plan stored off-site at alternate/backup locations? Copies of the contingency plan should be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the contingency plan that are stored in a private home must be protected from inadvertent access.

9. Required Resources

- Are the following resources for supporting critical operations defined and available for an emergency?
  - Hardware
  - Software
  - Communications
  - Data
  - Documents
  - Facilities
  - People
  - Supplies
  - Basic essentials (water, food, shelter, transportation, etc.)

- Does the contingency plan provide for backup personnel? As the contingency plan is implemented, it is necessary to have additional people available to support recovery operations. The contingency plan should specify who these people are and when they would normally be called into action.

10. Training

- Are management and staff trained to respond to emergencies? Security training should include modules for management and staff relative to their roles for handling emergency situations.

11. Testing the Contingency Plan

- Is there a section in the contingency plan that addresses testing of the plan?
- Testing of the contingency plan should address the following topics:
  - Test Philosophy
  - Test Plans
  - Boundaries
  - Live vs. Walkthrough vs. End-to-End Testing
  - Test Reports
  - Responsibilities

12. Contingency Plan Maintenance

- Schedule
  - Is the contingency plan annually reviewed and tested? The contingency plan should be reviewed and tested annually under conditions as close to an emergency as can be reasonably and economically simulated.
  - Is there a provision for updating the contingency plan annually?
  - Is the contingency plan revised after testing, depending on test results?

13. Relationships/Interfaces

- Does the contingency plan identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.

- Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?

- Is the plan compatible with plans of interacting organizations and systems?

- What internal interfaces must be considered?

- Is the plan compatible with plans of interacting organizations and systems?

- Which corporate interfaces must be considered?

- Are there special interfaces with corporate systems that must be addressed in the contingency plan?

14. Attachments

Does the contingency plan contain appropriate attachments, as listed below?

A. Actions for Each Phase

Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?

B. Procedures

- Are there detailed instructions for:
  - responding to emergencies?
  - recovering?
  - restoring operations?

- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency should be in place.

- Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?

- Is there an implementation plan for working from home?

C. Call Trees

Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?

D. Hardware Inventory

Are there lists of all the hardware covered by the contingency plan?

E. Software Inventory

Are there lists of all the software covered by the contingency plan?

F. System Descriptions

Are all the systems covered by the contingency plan defined, including appropriate diagrams?

G. Alternate/Backup Site Information

Is there sufficient detail to completely describe the alternate and/or backup sites, including addresses, phone numbers, contacts, resources available at the sites, *and* resources needed to be brought to the site?

H. Assets/Resources

Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary

Has there been a realistic assessment of the nature and size of the possible threat and of the resources most at risk?

J. Agreements/Memo of Understanding

Are there agreements in place relative to the use of alternate/backup sites, special resources, outside suppliers, extra people, alternate communications, etc?

K. Manual Operations

Are manual operating procedures in place so that certain functions can continue manually if automated support is not available soon enough?

Manual processing procedures should exist in the backup phase until automated capabilities can take over the information processing. Provisions should be made to provide this manual capability.

L. Supplies/Materials/Equipment

Is there information that describes how and where to obtain needed supplies, materials, and equipment?

M. Floor Plans

Are the necessary floor plans available?

N. Maps

Are the necessary area and street maps available?

12.0 - References

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- NIST Special Pub 800-34, Contingency Planning Guide for Information Technology Systems, June 2002. http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11.
  http://csrc.nist.gov/publications/nistpubs/800-12

- HCFA Program Memorandum, Business Continuity and Contingency Plans for Millennium Change, 12 August 1998.

- Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000.
  http://hipaa.ascensionhealth.org/infoexchange/disaster.html

- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, Section 3.6.
  http://www.gao.gov/special.pubs/12_19_6.pdf

- Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998.
  http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996.

http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Appendix C
An Approach to Fraud Control

Table of Contents
(Rev. 8, 04-06-07)

1.0 - Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This document develops countermeasures relating to fraudulent acts and a checklist to help Medicare contractors assess their vulnerability to fraud. Fraud and embezzlement *are* skyrocketing, largely because basic safeguards are neglected or lacking. Fraudulent acts are discussed in terms of the *types* of safeguards in place and functioning.

2.0 - Safeguards Against Employee Fraud

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These *safeguards* are consistent with the CMS CSRs outlined in Attachment A to this document and do not constitute wholly different or additional minimum requirements. The following countermeasures should prove especially effective against currently prevalent fraudulent activities and are discussed primarily as they relate to prevention *and* detection of fraud.

A. Screen New Employees

Screen new employees for positions that involve program funds directly or indirectly to address the applicant's past faithful and honest performance of duties with other employers in addition to job performance and investigation of his/her personal finances. New employees' statements concerning personal finances should be confirmed with former employers and with banking and credit institutions. Phone calls to previous employers are essential, particularly to former supervisors who should be advised of the nature of the position. Although former employers will sometimes fail to prosecute employees associated with fraudulent activities, they seldom delude a prospective employer asking about *the applicant's* integrity.

Any blatant dishonesty in the application (such as claiming qualifications and experience the applicant never had) should remove the applicant from further consideration. Check references and crosscheck them (one against the other) for consistency as well as content. Evaluate *references* on the basis of the contact's personal knowledge of the applicant's job-related qualifications and integrity.

Proper screening is preventive medicine at its best. Gaps in employment are flags that call for third-party verification, not just a plausible explanation by the applicant. Former employers may be able to shed light on the situation or be able to relate the reason given them about gaps by the applicant.

Circumstances relating to termination of previous employment should be clearly related by former employers. Resolve any inconsistencies or vagueness.

Ask former employers as well as the applicant, whether the employee was ever bonded, or was ever refused bonding. Sensitive screening should not result in violating an

applicant's civil rights, while assuring you (and your bonding company) that prudent concern is exercised in the hiring process.

B. Bonding

Bonding is also known as fidelity insurance and comes in all configurations; the broader the coverage, the more expensive the premium. One of the most important things you can do is analyze the extent and conditions of coverage in relation to possible *misappropriations of funds*. Liability is invariably limited in some respects. For example, coverage often does not extend to external fraud; to losses not proven to have been caused by fraudulent acts by covered employees; to frauds committed by employees known to have perpetrated dishonest acts previously; to frauds whose circumstances are not properly investigated; or to frauds whose alleged perpetrators are not brought to trial. Inherent in the analysis of bonding is risk analysis of fraud in relation to specific components to develop a worst-case fraud scenario in terms of dollar-loss before recovery through bonding.

C. Separation of Duties

Separate duties so that no one employee can defraud *the company* unaided. This is the cardinal rule for fraud prevention, one that is well-understood in manual operations. It is not as well understood in its application to computer processing where a single automated system may combine functions ordinarily separated, such as transactions and adjustments. Analyze all duties, including all stages of computer programming and operations, in terms of defeating single-handed fraud as well as in terms of effectiveness and efficiency, with fraud controls taking precedence. Group review of programmer cod*e* before allowing new/upgraded systems into production is the *type* of duty-separation (function vs. approval) that serves both effectiveness and security.

D. Rotation of Duties

Rotate duties, particularly those involving authorization of a transaction. Separation of duties makes it difficult for an employee to defraud your organization unaided, so that embezzlement becomes a crime of collusion. As more and more embezzlement involves more than one person, it becomes necessary to ensure that the same person is not always involved in approving another's functions. An employee is less likely to initiate a fraudulent transaction if he/she is not certain that his*/her* accomplice will be the one to approve or process that transaction. Moreover, the knowledge that *from time to time* other employees will perform his*/her* function or work his*/her* cases is a powerful deterrent to any fraudulent scheme, particularly embezzlement which requires continual cover-up.

E. Manual Controls

Manual controls are differentiated from automatic controls because constant review is necessary to see that they are in place and working. Moreover, they often supplement or augment automatic controls; for example, the manual review of claims rejected in computer processing. Review all manual controls to determine the extent to which they

would be effective against fraud in any operational area; too often, controls are reviewed without fraud specifically in mind. Classic manual controls are those associated with the tape/disk library, and these controls are strongly associated with restricted access and separation of duties. It does little good to separate programmer/operator duties if the programmer is allowed to sign out production tapes or master files for any reason, especially live-testing. Library controls should require specific authorization for tape removal for specific periods for specific reasons known to, and sanctioned by, the approving authority. The most important manual controls are those over blank-check stock and the automatic check-signer. The employee in control of the check-signer should not at the same time control the check stock, although these duties may be rotated so that the person controlling the check-signer one day may be assigned to control check stock on the following day when a third person is responsible for the check-signer. However, no one individual should be allowed to "sign" a check he/she has issued. Rotation of duties is proper only for subsequent operations where one's own previous actions have already cleared.

F. Training

Training employees in their responsibilities relative to fraud in their operations is basic to prudent management. This extends beyond the employee's own activities. For example, Title 18, U.S. Code Section 4 requires anyone having knowledge of a Federal crime to report it to the FBI or similar authority, with penalties of up to $500 fine and 3 years in jail for failure to do so. No employee should be ignorant of this responsibility. *This responsibility can be* explain*ed* as a simple good citizenship requirement and not spying or snitching. Discuss these things periodically in meetings, along with free give-and-take on moral issues and management's position on every aspect of fraud, including *perpetration involving* collusion with outsiders. Do not single out any employee or function in these discussions, instead make management's position clear regarding so-called "justification" for unauthorized "borrowing" and the fact that fraud can and will be prosecuted. Explain that there can be no permissive attitude towards dishonest acts because such an attitude is corrupting and makes it difficult for employees to remain honest. Make *it* known that there are controls throughout the organization to prevent and detect fraud, without being specific as to how they work. Require employees to report apparent loopholes in security that might one day (or already) be exploited for fraudulent purposes. Remind employees that ethical conduct requires their full cooperation in the event of any fraud investigation, and when interviewed they will be called upon to explain why security gaps or suspicious activities were not reported to the SSO. No security program can be effective without the involvement and cooperation of employees, and nowhere is this truer than with fraudulent activity.

G. Notices

Notices, both periodic and situational, are effective and necessary in the prevention and control of fraud. It is not enough to formulate management policy or to conduct employee training relative to fraudulent activity. It is possible to remind employees of management's continuing concerns and to evaluate employee awareness through simple reminders or announcements of what is happening relative to fraud controls (of a general

nature) and management's reliance on their cooperation and understanding of their responsibilities. Without this evidence of sustained management commitment, policy utterances tend to fade from memory or become regarded as part of a new employee's orientation and not part of the scene. This is true of minor abuses, but is also true of abuses that escalate into fraud.

H. Automatic Controls

Automatic controls to prevent or detect fraudulent activities comprise the first line of defense in computer operations. Such controls are often thought of as ensuring data integrity but more in terms of accuracy than of honesty. Evaluate automatic controls in terms of preventing payment to unauthorized persons. Test automatic controls with fraudulent (invalid) input, under strict control of course, and with management's full cognizance and prior approval.

I. Audit Routines

Audit routines are those programs where trained auditors test for fraud using special routines to reveal computer processing that creates or diverts payments to employees or their accomplices. Wrongdoers not only have to create bogus payments, but also *they* have to be able to lay their hands on the checks in order to cash them. Devise audit routines to single-out payments being directed to post office boxes or to repeat addresses (where such repeats would be unreasonable), to the addresses of an employee or his family, or to a drop-off address that is not a real business but merely a place to collect mail.

3.0 - Checklist for Medicare Fraud

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This checklist represents questions to address in analyzing the security of Medicare fiscal operations.

1) Have Medicare operations been identified where fraud or complicity in fraud may be possible, e.g. initiation/approval of payments?

2) Have individuals been assigned fraud-protection responsibilities in such components, including the responsibility for reporting possible fraud and vulnerability to fraud?

3) Do individual employees at all levels understand that management policy relative to fraud is dismissal and prosecution?

4) Are fiscal operations regularly audited relative to fraud vulnerability?

5) Are fraudulent acts specifically mentioned in the employee's code of ethical conduct?

6) Is employee integrity specifically addressed during the hiring process, and do background investigations elicit information that would uncover an applicant's past fraudulent activity with other employers?

7) Are operations set up in such a way as to discourage both individual and collusive fraudulent activity?

8) Are programs/systems tested by authorized individuals with “fraudulent” input?

9) Are audit trails generated that identify employees *who create* inputs or mak*e* adjustments/corrections that would pinpoint responsibility for any fraudulent act?

10) Is there an effective mechanism for detection/prevention of payments being purposely misdirected to employees, relatives, or accomplices?

11) Are new or changed programs specifically reviewed for fraudulent code by those responsible for production-run approval (persons empowered to review changes but not to make changes themselves)?

12) Are controls designed to prevent fraud, especially in those operations where large sums could be embezzled quickly?

13) Are all error-conditions checked for fraud potential?

14) Are balancing operations done creatively so that an embezzler could not hide discrepancies?

15) Are the official activities of all employees, at all levels, subject to independent review by different reviewers (i.e., not always by the same evaluator)?

16) Does management insist on integrity at all levels?

17) Has management announced that employee's work activities will be reviewed (in unspecified ways) for both the fact and appearance of integrity?

18) Do tape/disk library controls in fact prevent tampering with files/programs for fraudulent purposes?

19) Are alternative fraud controls invoked during emergencies?

20) Are suspected frauds investigated promptly and properly and are they thoroughly documented?

21) Are fraud audits conducted both periodically and randomly?

22) Are random samples taken of claims/bill inputs and checked back to their sources?

23) Does the Personnel *D*epartment check the applicant's background, employment record, references, and possible criminal record before hiring?

24) Are badges, I.D. #'s, and passwords promptly issued and rescinded?

25) Is off-hours work supervised, monitored, or otherwise effectively controlled?

26) Are all employees required to take their vacations and are their replacements required to check over the vacationers' past activities?

27) Are the credentials of outsiders, such as consultants and auditors, checked out?

28) Is temporary help bonded, hired from reputable agencies, and their activities restricted to the tasks to be performed? (Same principle applies to employees temporarily borrowed from non-Medicare components.)

29) Are written procedures controlled and restricted to employees currently assigned the relevant duties?

30) Are special fraud controls specified for backup operations?

31) Are incoming checks, including returned checks, handled by two or more individuals in the mailroom and are such teams switched around so that the same people are not always working together?

32) Are blank checks and automatic check-signing equipment strictly controlled with a tamper-proof numbering mechanism?

33) Is procedure/program documentation relative to the payment process treated as highly sensitive data and safeguarded when superseded?

34) Are backup files current and securely stored off-site?

Are re-runs checked for the possibility of fraud, especially duplicate payments?

Appendix D: - CMS Information Security Guidebook for Audits

(Rev. 8, 04-06-07)

1.0 - Introduction

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This guide has been developed to aid contractors in understanding and preparing for the various types of audits and reviews, which may be performed at their locations. Its purpose is to provide additional information on site selection criteria, audit steps and objectives, documentation requirements, the types of employees that will need to be interviewed, and space and equipment requirements for CFO audits, Section 912 Reviews, SAS 70 type II audits and Penetration/EVA testing.

1.1 - CFO/EDP Audit Acts

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The purpose of these audits is to ensure that proper IT controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for Centers for Medicare & Medicaid Services (CMS). The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.

A Chief Financial Officer (CFO) Act audit is conducted under the guidelines and supervision of the U.S. General Accountability Office (GAO). The GAO requires that all such audits follow the Federal Information Systems Control and Audit Manual (FISCAM). FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties. The FISCAM steps may be found on the GAO website at *http://www.gao.gov/aac.html* under the *Guidance* section.

1.2 - Section 912 Evaluation

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

As part of the Medicare Prescription Drug, Improvement and Modernization Act (MMA) of 2003, a requirement exists to perform an evaluation of the information security programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors must be in compliance with the eight statutory requirements set forth in the Federal Information Security Management Act (FISMA).

These evaluations are conducted according to procedures established by the Office of Information Services (OIS) with input from the U.S. Department of Health and Human Services, *Office of Inspector General (*OIG*)*. The procedures are organized using the eight FISMA statutory areas which include: periodic *R*isk *A*ssessments; policies and procedures based on *R*isk *A*ssessments that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the *S*ystems *D*evelopment *L*ife *C*ycle *(SDLC)* and complies with the National Institute of Standards and Technology (NIST) standards; System Security Plans; security awareness training; periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities; remedial activities, processes and reporting for deficiencies; incident detection, reporting and response, and continuity of operations for IT systems.

1.3 - SAS 70 Audits

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Statement on Auditing Standards (SAS) No. 70, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over IT and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 Audit.

1.4 - Penetration/EVA

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO's FISCAM dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal Government domain.

A network vulnerability assessment is the systematic examination of an information system to: determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.0 - Types of Audits

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

2.1 - CFO/EDP Audit Acts

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The purpose of these audits is to ensure that proper IT controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for Centers for Medicare and Medicaid Services (CMS). The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.

A Chief Financial Officer (CFO) Act audit is conducted under the guidelines and supervision of the U.S. GAO. The GAO requires that all such audits follow FISCAM. FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties. The FISCAM steps may be found on the GAO website at *http://www.gao.gov/aac.html* under the *Guidance* section.

One overall report is created for each site audited with the final report being issued by the OIG.

2.1.1 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Selection of sites to be included in the CFO Act audits is primarily based on the volume of claims processed, prior findings and significance of processing done. Smaller sites are rotated into the testing to ensure that their controls are also understood, but such sites are not likely to be audited every year. Because of the new requirements of the security evaluations set forth in Section 912 of the MMA (see section two of this guide for more detail), the need to rotate smaller sites into testing samples may diminish in the future.

2.1.2 - Audit Steps and Objectives

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The OIG of the Department of Health and Human Services performs audit work on the following areas of FISCAM during their audits:

Physical Access Controls

- AC-1 Classify information resources according to their criticality and sensitivity.
  - AC-1.1 Resource classifications and related criteria have been established.
  - AC-1.2 Owners have classified resources.

- AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
  - AC-3.1 Adequate physical security controls have been implemented.
    - AC-3.1.A Physical safeguards have been established that are commensurate with the risks of physical damage or access.
    - AC-3.1.B Visitors are controlled.
  - AC-3.4 *E*quipment and media *is sanitized* prior to disposal or reuse.

Entity Wide Security Program

- SP-1 Periodically assess risks.
  - SP-1.1 Risks are periodically assessed.

- SP-2 Document an entity wide security program plan.
  - SP-2.1 A security plan is documented and approved.
  - SP-2.2 The plan is kept current.

- SP-3 Establish a security management structure and clearly assign security responsibilities.
  - SP-3.1 A security management structure has been established.
  - SP-3.2 Information security responsibilities are clearly assigned.
  - SP-3.3 Owners and users are aware of security policies.
  - SP-3.4 An incident response capability has been implemented.

- SP-4 Implement effective security-related personnel policies.
  - SP-4.1 Hiring, transfer, termination, and performance policies address security.
  - SP-4.2 Employees have adequate training and expertise.

- SP-5 Monitor the security program's effectiveness and make changes as needed.
  - SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them.
  - SP-5.2 Management ensures that corrective actions are effectively implemented.

Segregation of Duties

- SD-1 Segregate incompatible duties and establish related policies.
  - SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties.
  - SD-1.2 Job descriptions have been documented.
  - SD-1.3 Employees understand their duties and responsibilities.

- SD-2 Establish access controls to enforce segregation of duties.
  - SD-2.1 Physical and logical access controls have been established.
  - SD-2.2 Management reviews effectiveness of control techniques.

- SD-3 Control personnel activities through formal operating procedures and supervision and review.
  - SD-3.1 Formal procedures guide personnel in performing their duties.
  - SD-3.2 Active supervision and review are provided for all personnel.

Service Continuity

- SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.
  - SC-1.1 Critical data and operations are identified and prioritized.
  - SC-1.2 Resources supporting critical operations are identified.
  - SC-1.3 Emergency processing priorities are established.

- SC-2 Take steps to prevent and minimize potential damage and interruption.
  - SC-2.1 Data and program backup procedures have been implemented.
  - SC-2.2 Adequate environmental controls have been implemented.
  - SC-2.3 Staff *has* been trained to respond to emergencies.
  - SC-2.4 Effective hardware maintenance, problem management, and change management *have been implemented to* prevent unexpected interruptions.

- SC-3 Develop and document a comprehensive contingency plan.
  - SC-3.1 An up-to-date contingency plan is documented.
  - SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.

- SC-4 Periodically test the contingency plan and adjust it as appropriate.

- SC-4.1 The plan is periodically tested.
- SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.

The CMS-contracted auditor performs audit work on the following areas of FISCAM as part of the CFO Act audits:

Access Controls

- AC-2 Maintain a current list of authorized users and their access authorized.
  - AC-2.1 Resource owners have identified authorized users and their access *is* authorized.
  - AC-2.2 Emergency and temporary access authorization is controlled.
  - AC-2.3 Owners determine disposition and sharing of data.

- AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
  - AC-3.2 Adequate logical access controls have been implemented. (see also EVA)
    - AC-3.2.A Passwords, tokens, or other devices are used to identify and authenticate users.
    - AC-3.2.B Identification of access paths.
    - AC-3.2.C Logical controls over data files and software programs.
    - AC-3.2.D Logical control over database*(s)*.
    - AC-3.2.E Logical controls over telecommunications access.
  - AC-3.3Cryptographic tools. (see also EVA)

- AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.
  - AC-4.1 Audit trails are maintained.
  - AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.
  - AC-4.3 Suspicious access activity is investigated and appropriate action is taken.

Application Software Development and Change Control

- CC-1 Processing features and program modifications are properly authorized.
  - CC-1.1 A system development life cycle methodology (SDLC) has been implemented.
  - CC-1.2 Authorizations for software modifications are documented and maintained.
  - CC-1.3 Use of public domain and person software is restricted.

- CC-2 Test and approve all new and revised software.
  - CC-2.1 Changes are controlled as programs progress through testing to final approval.
  - CC-2.2 Emergency changes are promptly tested and approved.
  - CC-2.3 Distribution and implementation of new or revised software is controlled.

- CC-3 Control software libraries
  - CC-3.1 Programs are labeled and inventoried.

- CC-3.2 Access to program libraries is restricted.
- CC-3.3 Movement of programs and data among libraries is controlled.

Systems Software

- SS-1 Limit access to systems software.
  - SS-1.1 Access authorizations are appropriately limited.
  - SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths.

- SS-2 Monitor access to and use of systems software.
  - SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.
  - SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.

- SS-3 Control systems software changes.
  - SS-3.1 Systems software changes are authorized, tested, and approved before implementation.

  SS-3.2 Installation of systems software is documented and reviewed.

2.1.3 - Testing Procedures

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Refer to Table *D*-2 in Section 3.0 of this appendix for detailed testing procedures.

2.1.4 - Documentation

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Documentation needed by the OIG for a CFO Act Audit usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

1. Entity-wide security programs (e.g., System Security Plan)

2. Network diagrams

3. *R*isk *A*ssessments and vulnerability analyses

4. Organizational charts which include names and titles for the Medicare, information systems, and information system security departments

5. *Self-Assessment with* Core Set of Security Requirements using the CMS Integrated Security Suite (CISS, formerly the Contractor Assessment Security Tool, a.k.a. "CAST")

6. Risk Assessment policies and any internal risk analysis documentation

7. Documentation on data and resource classification

8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations

9. The most recent SAS 70 and *R*isk *A*ssessment reports

10. Policies and procedures regarding conduct in the data center

11. Policies and procedures for back-up tape rotation and off-site storage

12. Policies and procedures for sanitation of media prior to disposal

13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms

14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas

15. Layout of company buildings and overview of operations in each building

16. Employee lists for Medicare, information systems, and information system security departments (lists should include: name or identification (ID) number, job title, department, start date, and position effective date)

17. Documentation of new hire information system security training program

18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas

19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract

20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests

21. Policies and procedures regarding the testing of the *disaster recovery* plan

22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable

23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

Documentation needed by the CMS-contracted auditor for a CFO Audit Act usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

Logical Access Controls

Information on logical access controls, including the following:
NOTE: Detailed reports will vary based on security software in use, i.e., RACF, Top Secret, ACF2, UNIX, NT, etc.

1. Security policies, standards, and procedures for:
   a. Creation, modification, and deletion of user-IDs, functional groups, etc.
   b. Periodic review of access
   c. Dial-up access
   d. Use and monitoring of emergency or temporary access (Fire-call IDs)
   e. Password composition/mask
   f. Violation and security monitoring
   g. Archiving, deleting, or sharing data files
   h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)

2. List of all terminations during the current fiscal year

3. List of all transfers during the current fiscal year

4. List of all new hires during the current fiscal year

5. List of all Medicare application users

6. List of all users with dial up access

7. List of all users with the ability to change security settings (administrators)

8. Access to access requests and authorizations (for a sample of users)

9. List of access request approvers

10. Documentation supporting recertification of users

11. List of emergency or temporary (fire-call) IDs

12. Activity log of emergency or temporary IDs

13. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties

14. System default password requirements

15. Use of generic, group, or system IDs

16. Database security requirements and settings

17. Security violation logging and monitoring

18. Evidence of review of user templates and/or profiles

19. Evidence of automatic timeout on terminals
20. Database access lists
21. Evidence supporting resolution of prior year audit findings

Systems Software

Systems Software information including:

1. Results of CA_EXAMINE runs
2. Policies and procedures for restricting access to systems software
3. A list of all system programmers
4. A list of all application programmers
5. A list of all computer operators
6. Results of the last review of system programmer access capabilities
7. A list of all vendor supplied software that indicates how current the software is
8. If available, integrity statements from vendors for all third party software
9. Policies and procedures for using and monitoring use of system utilities
10. Policies and procedures for identifying, selecting, installing and modifying systems software
11. Policies and procedures for disabling vender supplied defaults
12. Roles and responsibilities for system programmers
13. Policies and procedures for emergency software changes
14. A list of all systems software changes made during the fiscal year
15. A list of all emergency changes made during the fiscal year
16. A list of all current access to systems software
17. A list of all users with access to migrate programs to production
18. A sample of audit logs for system utilities and system programmer activity
19. Evidence of review of logs and follow up action taken

20. Initial Program Load (IPL) procedures

21. Log from last IPL

Application Development and Change Management

Information on change management, including the following:

1. System Development Life Cycle (SDLC) methodology document
2. A list of all changes made during the current fiscal year
3. Dates of and training materials from the most *recent SDLC training class*
4. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
5. A list of all authorized change request approvers
6. Policies and procedures over the use of personal and public domain software
7. Test plan standards
8. A log of ABENDS
9. Procedures for new software distribution
10. Policies and procedures for emergency changes
11. A list of all emergency changes during the current fiscal year
12. Identification of virus software in use
13. A list of all users with access to library management software
14. A list of all users with access to the production libraries (production code, source code, extra program copies)
15. Tape library logs for the most recent 3 months

2.1.5 - Interviews Required

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the Corrective Action Plan (CAP)
3. Person responsible for IT Risk Assessment

4. Person responsible for the System Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. Human resources (HR) contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. Local Area Network (LAN) administrator
11. Network (LAN) security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:
    a. Fiscal Intermediary Standard System (FISS)
    b. MultiCarrier System/Mandatory Claim Submission System (MCS)
    c. VIPS Medicare System (VMS)

2.1.6 - Space and Equipment Requirements

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Some of the requirements for space and equipment include the following:

1. Sufficient office space for eight people.
   a. The CMS-contracted auditor will have five people on site for the CFO Act audit – one site leader, three staff, and one security specialist.
   b. OIG will have three individuals onsite for the CFO Act audit.

2. At least five high-speed lines to connect to e-mail and share information.

Access to copier, fax machine, and printer.

2.2 - Section 912 Evaluation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

As part of the MMA, a requirement exists to perform an evaluation of the information security programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors must be in compliance with the eight statutory requirements set forth in the Federal Information Security Management Act (FISMA).

The CMS-contracted auditor has agreed to perform procedures established by CMS OIS and the U.S. Department of Health and Human Services, Office of Inspector General (OIG) associated with the eight FISMA statutory areas which include: Periodic risk assessments; Policies and procedures based on risk assessments that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the systems development life cycle and complies with the NIST standards; System Security Plans; Security awareness training; Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities; Remedial activities, processes and reporting for deficiencies; Incident detection, reporting and response; and, Continuity of operations for IT systems.

2.2.1 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

All Fiscal Intermediaries and Carriers are required to have a Section 912 evaluation annually.

2.2.2 - Audit Steps and Objectives

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Risk Assessments

1. Determine if the current system configuration is documented, including links to other systems.

2. Determine if *R*isk *A*ssessments are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.

3. Determine if data sensitivity and integrity of the data have been documented and if data have been classified.

4. Determine if threat sources, both natural and manmade, have been formally identified.

5. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.

6. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.

7. Determine if final risk determinations and related management approvals have been documented and maintained on file.

8. Determine if a mission/business impact analysis have been conducted and documented.

9. Obtain management's list of additional controls that have been identified to mitigate identified risks.

Policies and Procedures to Reduce Risk

1. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in the Risk Assessments section above.

2. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.

3. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.

4. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.

5. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.

6. Determine if security policies and procedures include controls to address platform security configurations and patch management.

Review of System Security Plans

1. Determine if a security plan is documented and approved.

2. Determine if the plan is kept current.

3. Determine if a security management structure has been established.

4. Determine if information security responsibilities are clearly assigned.

5. Determine if owners and users are aware of security policies.

6. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications

7. Determine if hiring, transfer, termination, and performance policies address security.

8. Determine if employee background checks are performed.

9. Determine if security employees have adequate security training and expertise.

10. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.

11. Determine if management ensures that corrective actions are effectively implemented.

Review of Security Awareness Training

1. Determine if employees have received a copy of the Rules of Behavior.

2. Determine if employee training and professional development has been documented and formally monitored.

3. Determine if there is mandatory annual refresher training for security.

4. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.

5. Determine if employees have received a copy of or have easy access to agency security procedures and policies.

6. Determine if security professionals have received specific training for their job responsibilities, and if the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.

Review of Periodic Testing and Evaluation of the Effectiveness of IT Security Policies

1. Determine if management reports *exist* for the review and testing of IT security policies and procedures, including network *R*isk *A*ssessment, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments.

2. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls *(*including logical and physical security controls, platform configuration standards, and patch management controls*)*.

3. Determine if remedial action is being taken for issues noted on audits.

Review of Remedial Activities, Processes, and Reporting for Deficiencies

1. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.

2. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.

3. Determine the number and nature of security IT weaknesses for which corrective action has been delayed, and determine if management *has* provided explanations as to why.

Review of Incident Detection, Reporting, and Response

1. Determine that management has processes *in place* to monitor systems and the network for unusual activity and/or intrusion attempts.

2. Determine if management has procedures *in place* to take *(*and has taken*)* action in response to unusual activity, intrusion attempts*,* and actual intrusions.

3. Determine that management processes and procedures include reporting of intrusion attempts and *actual* intrusions in accordance with FISMA guidance.

Policies and Procedures for Continuity of Operations and Related Physical Security Safeguards for IT Systems.

1. Determine if critical data and operations are formally identified and prioritized.

2. Determine if resources supporting critical operations are identified in contingency plans.

3. Determine if emergency processing priorities are established.

4. Determine if data and program backup procedures have been implemented.

5. Determine if adequate environmental controls have been implemented.

6. Determine if staff has been trained to respond to emergencies.

7. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.

8. Determine if policies and procedures for disposal of data and equipment exist and include applicable *f*ederal security and privacy requirements.

9. Determine if an up-to-date contingency plan is documented.

10. Determine if arrangements have been made for alternate data processing and telecommunications facilities.

11. Determine if the *contingency* plan is periodically tested.

12. Determine if the results are analyzed and *the* contingency plans *are* adjusted accordingly.

13. Determine if physical security controls exist to protect IT resources.

2.2.3 - Testing Procedures

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Refer to Table *D*-3 in section 3.0 of this appendix for detailed testing procedures.

2.2.4 - Documentation

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Documentation needed for Section 912 includes but is not limited to the following areas:

Risk Assessment Review

1. Current system configurations documentation including links to other systems
2. *R*isk *A*ssessments
3. Data classification policies/procedures
4. Threat source documentation (manmade/natural)
5. Documented system vulnerabilities, system flaws, or weaknesses
6. Risk determinations (assessments) w*ith* related management approvals
7. Mission/business impact analysis

Policies and Procedures

1. IT Security
2. Job descriptions for management

System Security Plan

1. *System* Security *P*lan
2. Security management structure
3. Information security job responsibilities
4. Hiring, termination, transfer policies/procedures
5. Background check policies/procedures
6. Security policy/procedure updates
7. Management review of corrective actions

Review of Security Awareness Training

1. Training/professional development policies/procedures
2. Training schedule (if applicable)
3. Awareness posters, booklets, newsletters, etc
4. List of security professionals (pick sample)

Review of Periodic Testing and Evaluation of the Effectiveness of IT Security Policies and Procedures including Network Assessments and Penetration Activities

1. Management reports for review *and* testing of IT security policies *and* procedures
2. Independent audit reports and evaluations

Review of Remedial Activities, Processed and Reporting for Deficiencies

1. Tracking of weaknesses (Database (DB), paper, etc)
2. Planned corrective actions
3. CAP
4. List of IT security weaknesses including dates of corrective actions

Review of Incident Detection, Reporting and Response

1. Policies/procedures for monitoring systems *and* the network
2. Policies/procedures for management response to unusual activity, intrusion attempts, and actual intrusions

Review of Policies and Procedures for Continuity of Operations and Related Physical Security Safeguards for IT Systems

1. Current Recovery Plan (COOP and DR)
2. Policies/procedures for continuity of operations and related physical security safeguards for IT systems
3. Testing results for contingency plans

2.2.5 - Interviews Required

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the CAP
3. Person responsible for IT Risk Assessment
4. Person responsible for the System Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. HR contact

8. Mainframe systems administrator
9. Mainframe security administrator
10. LAN administrator
11. LAN security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:
    a. FISS
    b. MCS
    c. VMS

2.2.6 - Space and Equipment Requirements

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

1. Sufficient office space for five people. The CMS-contracted auditor will have five people on site for the 912 review – One site leader and four staff

2. At least five high-speed lines to connect to e-mail and share information.

3. Access to copier, fax machine, and printer.

The first week will be for initial fieldwork and the second week will be to address any open items and complete follow-up work.

2.3 - SAS 70 Audits

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

SAS 70, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized because it *indicates* that a service organization has been through an in-depth audit of *IT* control activities *and* related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting firm. A formal report including the auditor's opinion (Service Auditor's Report) is issued to the service organization at the conclusion of a SAS 70 Audit.

2.3.1 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

SAS 70 covers scope and processing; therefore, the sites with the main processing centers will be rotated into the audit program.

2.3.2 - Audit Steps and Objectives

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The planned focus of the audit team is collecting information through inquiry, inspection, and observation.

The CMS-contracted auditor will assess the effectiveness of the controls in place as *indicated* by management's description of controls. Management's control objectives should be aligned with key FISCAM areas. These key areas include:

- Entity-wide Security Program
- Access Controls
- Control of Application Development and Implementation
- Systems Software
- Service Continuity
- Segregation of Duties

Typically the CMS-contracted auditor will assess the following (and other) control activities; contingent upon them being listed in management's description of controls:

A.1 An entity-wide security program has been documented, approved, and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure, clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness, and ensure security officer training and employee security awareness.

A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual, and temporary) and include termination and transfer procedures that require exit interviews, return of property (such as keys and ID cards), notification to security management of terminations, removal of access to systems, and escorting of terminated employees out of the facility.

A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.

A.4 Access to computerized applications, systems software, and Medicare data are appropriately authorized, documented and monitored, includes approval by resource

owners, procedures to control emergency and temporary access and procedures to share and properly dispose of data.

A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.

A.6 Physical access by all employees (including visitors) to Medicare facilities, data centers, and systems is appropriately authorized, documented, and access violations are monitored and investigated.

A.7 Medicare application and related systems software development and maintenance activities are authorized, documented, tested, and approved.

A.8 A System Development Life Cycle methodology is documented and in use and includes planning for and costs for security requirements in systems.

A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.

A.10 Access to program libraries is properly restricted, and movement of programs among libraries is controlled.

A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.

A.12 Activities of employees should be controlled via formal operating procedures that include monitoring of employee activities by management with documentation maintained to provide evidence of management's monitoring and review process.

A.13 A regular *R*isk *A*ssessment of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.

A.14 A centralized risk management focal point for IT *R*isk *A*ssessment has been established that includes promotion awareness programs, processes and procedures to mitigate risks and monitoring processes to assess the effectiveness of risk mitigation programs.

A.15 A risk assessment and System Security Plan has been documented, approved, and monitored by management in accordance with the CMS Risk Assessment and Systems Security Plan Methodologies.

A.16 Regularly scheduled processes required to support the Medicare contractor's continuity of operations (data, facilities or equipment) are performed.

A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial actions addressing findings noted from all security audits and reviews of IT systems, components and operations.

A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.

A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts, and actual intrusions.

A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the Federal Information Security Management Act (FISMA).

2.3.3 - Testing Procedures

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Please refer to Table *D*-4 in section 3.0 of this appendix for detailed testing procedures.

2.3.4 - Documentation

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Documentation needed for SAS 70 is specific to the control activities defined by management at each contractor site but may include the following:

1. Entity wide security programs (e.g., System Security Plan)
2. Network diagrams
3. *R*isk *A*ssessments and vulnerability analyses
4. Organizational charts that include names and titles for the Medicare, information systems, and information system security departments
5. Completed CSRs using the CISS
6. Risk Assessment policies and any internal risk analysis documentation
7. Documentation on data and resource classification
8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
9. The most recent SAS 70 and *R*isk *A*ssessment reports
10. Policies and procedures regarding conduct in the data center

11. Policies and procedures for back-up tape rotation and off-site storage

12. Policies and procedures for sanitation of media prior to disposal

13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms

14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas

15. Layout of company buildings and overview of operations in each building

16. Employee lists for Medicare, information systems, and information system security departments (lists should include: name or identification (ID) #, job title, department, start date, and position effective date)

17. Documentation of new hire/information system security training program

18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas

19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract

20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests

21. Policies and procedures regarding the testing of the plan

22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable

23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

24. Security policies, standards, and procedures for:
    a. Creation, modification, and deletion of user-IDs, functional groups, etc.
    b. Periodic review of access
    c. Dial-up access
    d. Use and monitoring of emergency or temporary access (Fire-call IDs)
    e. Password composition/mask
    f. Violation and security monitoring
    g. Archiving, deleting, or sharing data files
    h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)

25. List of all terminations during the current fiscal year

26. List of all transfers during the current fiscal year

27. List of all new hires during the current fiscal year

28. List of all Medicare application users

29. List of all users with dial up access

30. List of all users with the ability to change security settings (administrators)

31. Access to access requests and authorizations (for a sample of users)

32. List of access request approvers

33. Documentation supporting recertification of users

34. List of emergency or temporary (fire-call) IDs

35. Activity log of emergency or temporary IDs

36. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties

37. System default password requirements

38. Use of generic, group or system IDs

39. Database security requirements and settings

40. Security violation logging and monitoring

41. Evidence of review of user templates and/or profiles

42. Evidence of automatic timeout on terminals

43. Database access lists

44. Evidence supporting resolution of prior year audit findings

45. Results of CA_EXAMINE runs

46. Policies and procedures for restricting access to systems software

47. A list of all system programmers

48. A list of all application programmers

49. A list of all computer operators

50. Results of the last review of system programmer access capabilities

51. A list of all vendor supplied software indicating the current version of the software

52. If available, integrity statements from vendors for all third party software

53. Policies and procedures for using and monitoring use of system utilities

54. Policies and procedures for identifying, selecting, installing and modifying systems software

55. Policies and procedures for disabling vender supplied defaults

56. Roles and responsibilities for system programmers

57. Policies and procedures for emergency software changes

58. A list of all systems software changes made during the fiscal year

59. A list of all emergency changes made during the fiscal year

60. A list of all current access to systems software

61. A list of all users with access to migrate programs to production

62. A sample of audit logs for system utilities and system programmer activity

63. Evidence of review of logs and follow up action taken

64. Initial Program Load (IPL) procedures

65. Log from last IPL

66. System Development Life Cycle (SDLC) methodology document

67. Change control policies and procedures (if not included in the SDLC document)

68. A list of all changes made during the current fiscal year

69. Dates of and training materials from the most recent SDLC training class

70. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)

71. A list of all authorized change request approvers

72. Policies and procedures over the use of personal and public domain software:

73. Test plan standards

74. A log of abends

75. Procedures for new software distribution

76. Policies and procedures for emergency changes

77. A list of all emergency changes during the current fiscal year

78. Identification of virus software in use

79. A list of all users with access to library management software

80. A list of all users with access to the production libraries (production code, source code, extra program copies)

81. Tape library logs for the most recent 3 months

82. Current system configurations documentation including links to other systems

83. Threat source documentation (manmade/natural)

84. Documented system vulnerabilities, system flaws or weaknesses

85. Mission/business impact analysis

86. Job descriptions for management

87. Information security job responsibilities

88. Background check policies/procedures

89. Security policy/procedure updates

90. Management review of corrective actions

91. Training/professional development policies/procedures

92. Training schedule (if applicable)

93. Awareness posters, booklets, newsletters, etc

94. Management reports for review & testing of IT security policies & procedures

95. Independent audit reports and evaluations

96. Tracking of weaknesses (DB, paper, etc)

97. Planned corrective actions

98. CAP

99. List of IT security weaknesses including dates of corrective actions

100. Policies/procedures for monitoring systems & the network

101. Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions

2.3.5 - Interviews Required

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the CAP
3. Person responsible for IT Risk Assessment
4. Person responsible for the System Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. HR contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. LAN administrator
11. LAN security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:
    a. FISS
    b. MCS
    c. MS

2.3.6 - Space and Equipment Requirements

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

1. Sufficient office space for six people. The CMS-contracted auditor will have six people on site for the SAS 70 audit – Four staff (senior associate/associate), one expert, and one manager

2. At least six high-speed lines to connect to e-mail and share information.

3. Access to copier, fax machine, and printer.

The CMS-contracted auditor auditors shall stay six weeks over a 3-4 month period to complete the audit.

2.4 - Penetration/EVA

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO FISCAM, dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal Government domain.

For purposes of this engagement, a network vulnerability assessment is the systematic examination of an information system, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.4.1 - Execution of the Audit

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results. The testing includes procedures to demonstrate both external and internal threats. To ensure that the integrity of the testing is not impaired, parties with knowledge of the testing are requested to restrict communicating any aspects, including test schedules to individuals at the operational level prior to or during test performance.

The CMS-contracted auditor is the Independent Public Accountant (IPA) engaged by the OIG Department of Health and Human Services (HHS) to perform testing at third party CMS contractors as part of the FY 2004 Financial Statement Audit of the Centers for Medicare and Medicaid Services ("CMS").

There will be a site summary that includes a high level description of the testing performed and findings describing technical issues identified during testing. The findings will be written in terms of Condition, Cause, Criteria, Effect, and Recommendation (following GAO Yellow Book guidelines). The Site Summary will be supported by summary work papers for each type of testing performed.

2.4.2 - Site Selection Criteria
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Sites are included in the CFO Act audits primarily based on the volume of claims processed, prior findings and significance of processing done. Smaller sites are rotated into the testing to ensure that their controls are also understood, but such sites are not likely to be audited every year.

2.4.3 - Audit Steps and Objectives
(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Steps to perform penetration testing

Phase 1 – Assess & Model Threats

The Assess & Model Threats phase is used to establish and acquire the information required to successfully define the scope of the security penetration testing. This involves gathering information and completing an initial threat analysis to ensure that testing emulates the threats that are of real concern to the organization. This includes project start-up, information gathering and threat analysis.

1. Threat analysis is usually conducted according to prescribed scenarios that are clearly documented in the Statement of Work. Some common threat scenarios for an external penetration test include:

    a. Untrusted Outsider – This is the most common scenario for an External (Internet) penetration test. This scenario is designed to simulate individuals with no significant knowledge of the client's computing operations that are attempting to gain access from remote locations;

    b. Trusted Outsider – This scenario is designed to simulate third parties (e.g., customers, suppliers, partners) that have limited legitimate access to the client's network. In the event of the trusted outsider scenario, establish with the client what resources the team will attack and arrange for the client to set up valid credentials to access those resources (e.g., usernames/passwords, SecurID tokens).

2. During the project start-up, agree on primary contacts for both the CMS-contracted auditor and the client to contact in case of an emergency. These contact numbers should be accessible at all times during testing. All members of the team should be aware of the escalation path and procedures during testing.

3. Determine with the client when testing should stop. Some clients request that as soon as access is obtained, the CMS-contracted auditor stop and notify the client before attempting to obtain further access to resources.

4. Determine if there are specific targets of interest that the CMS-contracted auditor should direct attacks to (e.g., a focus on the client's web server).

5. All penetration activities must be conducted from either a CMS-contracted auditor lab or the client site. Identify the source IP range you will be using with the client to allow them to differentiate the CMS-contracted auditor activities from legitimate hacking attempts. Contact your lab manager for information on your external IP address range.

6. Establish acceptable timeframes for penetration testing with the client to avoid disrupting day-to-day client business (and to avoid being caught if the engagement requires stealth testing).

7. Inquire about any IP addresses that should be excluded from testing.

Phase 2 – Survey Testing

The Survey Testing phase is used to identify and document client devices that may be accessed from the Internet and to determine if any of these devices might be vulnerable to well-known exploits. This includes gathering IP address, MAC address, operating system, Web server, application, and enticement information, in addition to any other salient information about the target environment.

1. Identify Internet connections and IP ranges by querying public databases.

2. Identify salient target information available in newsgroups and web pages.

3. Use DNS queries to identify client networks and systems. These queries are best performed from a UNIX system that has the dig utility installed (NOTE: dig is also available for Windows systems). IP addresses that are found through DNS queries should be looked up in the Internet repositories listed above to determine the range and owner of the IP address. The following queries can be used to identify client systems and networks:

4. Once you have identified client IP ranges and accessible websites, confirm IP addresses with the client contact before attempting to attack any systems.

    a. Once the client has approved the IP ranges identified during the first part of this phase, scans can be conducted using a map to identify open ports and potential attack points on each of the servers in the range. Depending on the requirements of the organization, different types of scans may be used to try and avoid detection.

5. Once the initial scan is complete, a table should be created for the information gathered from each port.

6. After you have identified the services running on each port and obtained all information possible, the Intrusion Testing Phase of the engagement can begin. Note: confirm with the engagement manager before beginning Intrusion testing to determine if the client needs to be notified before beginning.

Phase 3 – Intrusion Testing

The Intrusion Testing phase is used to examine the weaknesses found and, where appropriate, attempt to exploit these weaknesses to demonstrate the risks and exposures. This stage is the core

of the security penetration test and may be an iterative process as one exploited weakness may give rise to further exploitation opportunities.

The overall goal of the Intrusion Testing phase is to demonstrate access to systems and the capability to exploit this access further, not necessarily to gain full uncontrolled access to systems, although there may be instances where such access may be permissible.

1. Each attempt you make to gain access to systems (including every username and password combination) **must be documented**. There are an infinite number of avenues to attempt to gain access to a system, but the intrusion attempts should be performed in the following order.

2. If you gain access to a system, **take a screen shot** and **SLOW DOWN**.

2. Navigate the filesystem and attempt to identify any sensitive data files. These may include usernames, passwords or SMTP strings.

4. Use the machine as a "stepping stone" and exploit any trust relationships to compromise additional machines. Determine any network interfaces this system has (e.g., network interface cards) and determine what capabilities the system gives you (e.g., ping internally, telnet). Further system testing, such as this, should be conducted according to the same procedures prescribed so far: (1) Assess and Model Threats; (2) Survey Testing; and (3) Intrusion Testing.

Phase 4 – Assess Exposures

Throughout the assessment, the practitioner should consistently document any actions and findings. The assess exposures phase (reporting phase) brings together this information in a presentable format and draws conclusions about the impact of each finding to the business. This stage requires an analysis of the data to provide actionable, reasonable information to the client.

2.4.4 - Documentation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Documentation and other items needed for Penetration/External Vulnerability Assessment (EVA) includes, but is not limited to:

1. Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.

2. Site / system password policies

3. Applicable phone number range for dial-up "war-dialing" testing.

4. Applicable Internet Protocol (IP) address spaces for penetration testing.

5. Listing of IP addresses assigned to, or under the purview of the site.

6. Listing of prohibited telephones/systems/networks

7. Standards and Guidelines (Risk Model) for system configuration.

Additional Penetration/EVA items include:

1. Personnel to observe the penetration and diagnostic testing activities (if desired by the auditee).

2. Permission to connect the CMS-contracted auditor laptop to site's network (while monitored).

3. Network access for internal testing.

System administrator/programmer access for systems to perform diagnostic review.

4. Specific documents required by the CMS-contracted auditor will be requested in the Provided by Client (PBC) list. This list will be provided prior to the start of testing.

2.4.5 - Interviews Required

(Rev.6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

1. An individual from the Security Department

2. CMS Contact

3. Someone knowledgeable of the CMS environment

4. Systems Administrator

5. Network Administrator

6. Database Administrator

7. Firewall Administrator

2.4.6 - Space and Equipment Requirements

(Rev.6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

1. Workspace for each member of the audit team – usually one Senior Associate and one Associate

2. At least 1 telephone line, and network connectivity.

The CMS-contracted auditor auditors will typically stay 3-5 days, depending upon the readiness of the contractor.

3.0 - Tables

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This table provides a synopsis of required documentation.

Table D-1. Synopsis of Documentation Required

Documentation	CFO Audit	Section 912	SAS 70	EVA
Entity wide security programs (e.g., System Security Plan)	✔	✔	✔	
Network diagrams	✔	✔	✔	✔
*R*isk *A*ssessments and vulnerability analyses	✔	✔	✔	
Organizational charts which include names and titles for the Medicare, information systems, and information system security departments	✔	✔	✔	
Completed CSRs using the CISS	✔	✔	✔	
Risk Assessment policies and any internal risk analysis documentation	✔	✔	✔	
Documentation on data and resource classification	✔	✔	✔	
HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations	✔	✔	✔	
The most recent SAS 70 and *R*isk *A*ssessment reports	✔		✔	
Policies and procedures regarding conduct in the data center	✔		✔	
Policies and procedures for back-up tape rotation and off-site storage	✔	✔	✔	
Policies and procedures for sanitation of media prior to disposal	✔	✔	✔	
Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms	✔		✔	
Policies and procedures regarding visitors to both the general campus and to the sensitive areas	✔		✔	
Layout of company buildings and overview of operations in each building	✔		✔	
Employee lists for Medicare, information systems, and information system security departments (lists should include: name or identification (ID) #, job title, department, start date, and position effective date)	✔	✔	✔	
Documentation of new hire/information system security training program	✔	✔	✔	
Vendor sign in and sign out logs for maintenance or repairs in sensitive areas	✔		✔	
Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract	✔		✔	
Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.	✔	✔	✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Policies and procedures regarding the testing of the plan	✔	✔	✔	
Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable	✔	✔	✔	
Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan	✔	✔	✔	
Security policies, standards, and procedures for:				
• Creation, modification, and deletion of user-IDs, functional groups, etc.	✔		✔	
• Periodic review of access	✔		✔	
• Dial-up access	✔		✔	
• Use and monitoring of emergency or temporary access (Fire-call IDs)	✔		✔	
• Password composition/mask	✔		✔	✔
• Violation and security monitoring	✔		✔	
• Archiving, deleting, or sharing data files	✔		✔	
• Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)	✔		✔	
List of all terminations during the current fiscal year	✔		✔	
List of all transfers during the current fiscal year	✔		✔	
List of all new hires during the current fiscal year	✔		✔	
List of all Medicare application users/	✔	✔	✔	
List of all users with dial up access	✔		✔	
List of all users with the ability to change security settings (administrators)	✔		✔	
Access to access requests and authorizations (for a sample of users)	✔		✔	
List of access request approvers	✔		✔	
Documentation supporting recertification of users	✔		✔	
List of emergency or temporary (fire-call) IDs	✔		✔	
Activity log of emergency or temporary IDs	✔		✔	
Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties	✔		✔	
System default password requirements	✔		✔	
Use of generic, group or system IDs	✔		✔	
Database security requirements and settings	✔		✔	
Security violation logging and monitoring	✔		✔	
Evidence of review of user templates and/or profiles	✔		✔	
Evidence of automatic timeout on terminals	✔		✔	
Database access lists	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Evidence supporting resolution of prior year audit findings	✔		✔	
Results of CA_EXAMINE runs	✔		✔	
Policies and procedures for restricting access to systems software	✔		✔	
A list of all system programmers	✔		✔	
A list of all application programmers	✔		✔	
A list of all computer operators	✔		✔	
Results of the last review of system programmer access capabilities	✔		✔	
A list of all vendor supplied software that indicates how current the software is	✔		✔	
If available, integrity statements from vendors for all third party software	✔		✔	
Policies and procedures for using and monitoring use of system utilities	✔		✔	
Policies and procedures for identifying, selecting, installing and modifying systems software	✔		✔	
Policies and procedures for disabling vender supplied defaults	✔		✔	
Roles and responsibilities for system programmers	✔		✔	✔
Policies and procedures for emergency software changes	✔		✔	
A list of all systems software changes made during the fiscal year	✔		✔	
A list of all emergency changes made during the fiscal year	✔		✔	
A list of all current access to systems software	✔		✔	
A list of all users with access to migrate programs to production	✔		✔	
A sample of audit logs for system utilities and system programmer activity	✔		✔	
Evidence of review of logs and follow up action taken	✔		✔	
Initial Program Load (IPL) procedures	✔		✔	
Log from last IPL	✔		✔	
System Development Life Cycle (SDLC) methodology document	✔	✔	✔	
Change control policies and procedures (if not included in the SDLC document)	✔		✔	
A list of all changes made during the current fiscal year	✔		✔	
Dates of and training materials from the most recent SDLC training class	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)	✔		✔	
A list of all authorized change request approvers	✔		✔	
Policies and procedures over the use of personal and public domain software:	✔		✔	
Test plan standards	✔		✔	
A log of ABENDS	✔		✔	
Procedures for new software distribution	✔		✔	
Policies and procedures for emergency changes	✔		✔	
A list of all emergency changes during the current fiscal year	✔		✔	
Identification of virus software in use	✔		✔	
A list of all users with access to library management software	✔		✔	
A list of all users with access to the production libraries (production code, source code, extra program copies)	✔		✔	
Tape library logs for the most recent 3 months	✔		✔	
Current system configurations documentation including links to other systems		✔	✔	
Threat source documentation (manmade/natural)		✔	✔	
Documented system vulnerabilities, system flaws or weaknesses		✔	✔	
Mission/business impact analysis		✔	✔	
Job descriptions for management		✔	✔	
Information security job responsibilities		✔	✔	
Background check policies/procedures		✔	✔	
Security policy/procedure updates		✔	✔	
Management review of corrective actions		✔	✔	
Training/professional development policies/procedures		✔	✔	
Training schedule (if applicable)		✔	✔	
Awareness posters, booklets, newsletters, etc		✔	✔	
Management reports for review & testing of IT security policies & procedures		✔	✔	
Independent audit reports and evaluations		✔	✔	
Tracking of weaknesses (DB, paper, etc)		✔	✔	
Planned corrective actions		✔	✔	
All four quarter CAPs		✔	✔	
List of IT security weaknesses including dates of corrective actions		✔	✔	
Policies/procedures for monitoring systems & the network		✔	✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions		✔	✔	
Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.				✔
Standards and Guidelines (Risk Model) for system configuration.				✔
Applicable phone number range for dial-up “war-dialing” testing.				✔
Applicable Internet Protocol (IP) address spaces for penetration testing.				✔
Listing of IP addresses assigned to, or under the purview of the site.				✔
Listing of prohibited telephones/systems/networks				✔

Table D-2. Detailed CFO Testing Procedures

Control Activity	Detailed Testing
Access Control	
AC-1 Classify information resources according to their criticality and sensitivity.	
1. Resource classifications and related criteria have been established.	1. Review policies and procedures. 2. Interview resource owners.
2. Owners have classified resources.	1. Review resource classification documentation and compare to *R*isk *A*ssessments. Discuss any discrepancies with appropriate officials.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.	
1. Adequate physical security controls have been implemented.	
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Review a diagram of the physical layout of the computer, telecommunications, and cooling system facilities. 2. Walk through facilities. 3. Review risk analysis. 4. Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access. 5. Before becoming recognized as the auditor, attempt to access sensitive areas without escort or identification badges. 6. Observe entries to and exits from facilities during and after normal business hours. 7. Observe utilities access paths. 8. Interview management. 9. Observe entries to and exits from sensitive areas during and after normal business hours. 10. Interview employees. 11. Review procedures for the removal and return of storage media from and to the library. 12. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement. 13. Observe practices for safeguarding keys and other devices. 14. Review written emergency procedures. 15. Examine documentation supporting prior fire drills. 16. Observe a fire drill.
B. Visitors are controlled.	1. Review visitor entry logs. 2. Observe entries to and exits from sensitive areas during and after normal business hours. 3. Interview guards at facility entry. 4. Review documentation on and logs of entry code changes.

Control Activity	Detailed Testing
	5. Observe appointment and verification procedures for visitors.
2. Sanitation of equipment and media prior to disposal or reuse.	1. Review written procedures.
	2. Interview personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, test that they have been appropriately sanitized.
Entity Wide Security Program	
SP-1 Risks are periodically assessed.	
1. Risks are periodically assessed.	1. Review *R*isk *A*ssessment policies.
	2. Review the most recent high-level *R*isk *A*ssessment.
	3. Review the objectivity of personnel who performed and reviewed the assessment.
SP-2 Document an entitywide security program plan.	
1. A security plan is documented and approved.	1. Review the security plan.
	2. Determine whether the plan covers the topics prescribed by OMB Circular A-130.
2. The plan is kept current.	1. Review the security plan and any related documentation indicating that it has been reviewed and updated and is current.
SP-3 Establish a security management structure and clearly assign security responsibilities.	
1. A security management structure has been established.	1. Review the security plan and the entity's organization chart.
	2. Interview security management staff.
	3. Review pertinent organization charts and job descriptions.
	4. Interview the security manager.
2. Information security responsibilities are clearly assigned.	1. Review the security plan.
3. Owners and users are aware of security policies.	1. Review documentation supporting or evaluating the awareness program. Observe a security briefing.
	2. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
	3. Review memos, electronic mail files, or other policy distribution mechanisms.
	4. Review personnel files to test whether security awareness statements are current.
	5. Call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.

Control Activity	Detailed Testing
4. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.
	2. Review documentation supporting incident handling activities.
	3. Determine qualifications of response team members.
SP-4 Implement effective security-related personnel policies.	
1. Hiring, transfer, termination, and performance policies address security.	1. Review hiring policies.
	2. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
	3. Review reinvestigation policies.
	4. For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed.
	5. Review policies on confidentiality or security agreements.
	6. For a selection of such users, determine whether confidentiality or security agreements are on file.
	7. Review vacation policies.
	8. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	9. Determine who performed vacationing employee's work during vacation.
	10. Review job rotation policies.
	11. Review staff assignment records and determine whether job and shift rotations occur.
	12. Review pertinent policies and procedures.
	13. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.
	14. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Employees have adequate training and expertise.	1. Review job descriptions for security management personnel, and for a selection of other personnel.
	2. For a selection of employees, compare personnel records on education and experience with job descriptions.
	3. Review training program documentation.
	4. Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.

Control Activity	Detailed Testing
SP-5 Monitor the security program's effectiveness and make changes as needed.	
1. Management periodically assesses the appropriateness of security policies and compliance with them.	1. Review the reports resulting from recent assessments, including the most recent FMFIA report.
	2. Determine when the last independent review or audit occurred and review the results.
	3. Review written authorizations or accreditation statements.
	4. Review documentation related to corrective actions.
2. Management ensures that corrective actions are effectively implemented.	1. Review the status of prior-year audit recommendations and determine if implemented corrective actions have been tested.
	2. Review recent FMFIA reports.
Segregation of Duties	
SD-1 Segregate incompatible duties and establish related policies.	
1. Incompatible duties have been identified and policies implemented to segregate these duties.	1. Review pertinent policies and procedures.
	2. Interview selected management and information security personnel regarding segregation of duties.
	3. Review an agency organization chart showing information security functions and assigned personnel.
	4. Interview selected personnel and determine whether functions are appropriately segregated.
	5. Determine whether the chart is current and each function is staffed by different individuals.
	6. Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained.
	7. Observe activities of personnel to determine the nature and extent of compliance with the intended segregation of duties.
	8. Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combination of functions.
	9. Interview management, observe activities, and test transactions.
	10. Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	11. Review the adequacy of documented operating procedures for the data center.
2. Job descriptions have been documented.	1. Review job descriptions for several positions in organizational units and for user security administrators.
	2. Determine whether duties are clearly described and prohibited activities are addressed.

Control Activity	Detailed Testing
	3. Review the effective dates of the position descriptions and determine whether they are current.
	4. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	5. Review job descriptions and interview management personnel.
3. Employees understand their duties and responsibilities.	1. Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	2. Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	3. Interview management personnel in these activities.
SD-2 Establish access controls to enforce segregation of duties.	
1. Physical and logical access controls have been established.	1. Interview management and subordinate personnel.
2. Management reviews effectiveness of control techniques.	1. Interview management and subordinate personnel.
	2. Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	3. Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review the results of such reviews.
SD-3 Control personnel activities through formal operating procedures and supervision and review.	
1. Formal procedures guide personnel in performing their duties.	1. Review manuals.
	2. Interview supervisors and personnel.
	3. Observe processing activities.
2. Active supervision and review are provided for all personnel.	1. Interview supervisors and personnel.
	2. Observe processing activities.
	3. Review history log reports for signatures indicating supervisory review.
	4. Determine who is authorized to perform the initial program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.
Service Continuity	

Control Activity	Detailed Testing
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.	
1. Critical data and operations are identified and prioritized.	1. Review related policies.
	2. Review list and any related documentation.
	3. Interview program, data processing, and security administration officials. Determine their input and their assessment of the reasonableness of priorities established.
2. Resources supporting critical operations are identified.	1. Review related documentation.
	2. Interview program and security administration officials.
3. Emergency processing priorities are established.	1. Review related policies.
	2. Review related documentation.
	3. Interview program and security administration officials.
SC-2 Take steps to prevent and minimize potential damage and interruption.	
1. Data and program backup procedures have been implemented.	1. Review written policies and procedures for backing up files.
	2. Compare inventory records with the files maintained off-site and determine the age of these files.
	3. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports.
	4. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	5. Locate and examine documentation.
	6. Examine the backup storage site.
2. Adequate environmental controls have been implemented.	1. Examine the entity's facilities
	2. Interview site managers.
	3. Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observe the operation, location, maintenance and access to the air-cooling system.
	5. Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determine whether the activation of heat and smoke detectors will notify the fire department.
	7. Review test policies.

Control Activity	Detailed Testing
	8. Review documentation supporting recent tests of environmental controls.
	9. Review policies and procedures regarding employee behavior.
	10. Observe employee behavior.
3. Staff has been trained to respond to emergencies.	1. Interview data center staff.
	2. Review training records.
	3. Review training course documentation.
	4. Review emergency response procedures.
	5. Review test policies.
	6. Review test documentation.
	7. Interview data center staff.
4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	1. Review policies and procedures.
	2. Interview data processing and user management.
	3. Review maintenance documentation.
	4. Interview data center management.
	5. Interview senior management, data processing management, and user management.
	6. Review supporting documentation.
SC-3 Develop and document a comprehensive contingency plan.	
1. An up-to-date contingency plan is documented.	1. Review the contingency plan and compare its provisions with the most recent *R*isk *A*ssessment and with a current description of automated operations.
	2. Interview senior management, data center management, and program managers.
	3. Review the contingency plan.
	4. Interview senior management, data center management, and program managers.
	5. Observe copies of the contingency plan held off-site.
	6. Review the plan and any documentation supporting recent plan reassessments.
2. Arrangements have been made for alternate data processing and telecommunications facilities.	1. Review contracts and agreements.
SC-4 Periodically test the contingency plan and adjust it as appropriate.	
1. The plan is periodically tested.	1. Review policies on testing.
	2. Review test results.
	3. Observe a disaster recovery test.
2. Test results are analyzed and contingency plans are adjusted accordingly.	1. Review final test report.
	2. Interview senior managers to determine if they are aware of the test results.
	3. Review any documentation supporting contingency plan adjustments.

The CMS-contracted auditor will perform audit work on the following areas of FISCAM as part of the CFO Act audits:

Control Activity	Detailed Testing
Access Controls	
AC-2 Maintain a current list of authorized users and their access authorized.	
1. Resource owners have identified authorized users and their access authorized.	1. Review pertinent written policies and procedures.
	2. For a selection of users (both application user and information security personnel) review access authorization documentation.
	3. Interview owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, review authorization and justification.
	5. Interview security managers and review documentation provided to them.
	6. Review a selection of recent profile changes and activity logs.
	7. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Review pertinent policies and procedures.
	2. Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.
	3. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examine standard approval forms.
	2. Interview data owners.
	3. Examine documents authorizing file sharing and file sharing agreements.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.	
1. Adequate logical access controls have been implemented. (see also EVA)	
A. Passwords, tokens, or other devices are used to identify and authenticate users.	1. Review pertinent policies and procedures.
	2. Interview users.
	3. Review security software password parameters.
	4. Observe users keying in passwords.
	5. Attempt to log on without a valid password; make repeated attempts to guess passwords.
	6. Assess procedures for generating and communicating passwords to users.

Control Activity	Detailed Testing
	7. Review a system-generated list of current passwords.
	8. Search password file using audit software.
	9. Attempt to log on using common vendor supplied passwords.
	10. Interview users and security managers.
	11. Review a list of IDs and passwords.
	12. Repeatedly attempt to log on using invalid passwords.
	13. Review security logs.
	14. Review pertinent policies and procedures.
	15. Review documentation of such comparisons.
	16. Interview security managers.
	17. Make comparison using audit software.
	18. View dump of password files (e.g., hexadecimal printout).
	19. Interview users.
	20. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.
B. Identification of access paths.	1. Review access path diagram.
C. Logical controls over data files and software programs.	1. Interview security administrators and system users.
	2. Review security software parameters.
	3. Observe terminals in use.
	4. Review a system-generated list of inactive logon IDs, and determine why access for these users has not been terminated.
	5. Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Perform penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system. These tests should be performed as (1) an "outsider" with no information about the entity's computer systems; and (2) an "outsider" with prior knowledge about the systems--e.g., an ex-insider, and (3) an "insider" with and without specific information about the entity's computer systems, and with access to the entity's facilities.

Control Activity	Detailed Testing
	7. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
	8. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determine whether naming conventions are used.
D. Logical controls over a database.	1. Review pertinent policies and procedures.
	2. Interview database administrator.
	3. Review DBMS and DD security parameters.
	4. Test controls by attempting access to restricted files.
	5. Review security system parameters.
E. Logical controls over telecommunications access.	1. Review pertinent policies and procedures.
	2. Review parameters set by communications software or teleprocessing monitors.
	3. Test telecommunications controls by attempting to access various files through communications networks.
	4. Identify all dial-up lines through automatic dialer software routines and compare with known dial-up access. Discuss discrepancies with management.
	5. Interview telecommunications management staff and users.
	6. Review pertinent policies and procedures.
	7. View the opening screen seen by telecommunication system users.
	8. Review the documentation showing changes to dial-in numbers.
	9. Review entity's telephone directory to verify that the numbers are not listed.
2. Cryptographic tools. (see also EVA)	1 To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.	
1. Audit trails are maintained.	1. Review security software settings to identify types of activity logged.
2. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Review pertinent policies and procedures.
	2. Review security violation reports.
	3. Examine documentation showing reviews of questionable activities.

Control Activity	Detailed Testing
3. Suspicious access activity is investigated and appropriate action is taken.	1. Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator.
	2. Interview senior management and personnel responsible for summarizing violations.
	3. Review any supporting documentation.
	4. Review policies and procedures and interview appropriate personnel.
	5. Review any supporting documentation.
Application Software Development and Change Control	
CC-1 Processing features and program modifications are properly authorized.	
1. A system development life cycle methodology (SDLC) has been implemented.	1. Review SDLC methodology.
	2. Review system documentation to verify that SDLC methodology was followed.
	3. Interview staff.
	4. Review training records.
2. Authorizations for software modifications are documented and maintained.	1. Identify recent software modifications and determine whether change request forms were used.
	2. Examine a selection of software change request forms for approvals.
	3. Interview software development staff.
3. Use of public domain and person software is restricted.	1. Review pertinent policies and procedures.
	2. Interview users and data processing staff.
CC-2 Test and approve all new and revised software.	
1. Changes are controlled as programs progress through testing to final approval.	1. Review test plan standards.
	2. For the software change requests selected for control activity CC-1.2: (1) review specifications; (2) trace changes from code to design specifications; (3) review test plans; (4) compare test documentation with related test plans; (5) analyze test failures to determine if they indicate ineffective software testing; (6) review test transactions and data.
	3. For the software change requests selected for control activity CC-1.2 (continued): (1) review test results; (2) review documentation of management or security administrator reviews; (3) verify user acceptance; and (4) review updated documentation.
	4. Determine whether operational systems experience a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
2. Emergency changes are promptly tested and approved.	1. Review procedures.
	2. For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.

Control Activity	Detailed Testing
3. Distribution and implementation of new or revised software is controlled.	1. Examine procedures for distributing new software. 2. Examine implementation orders for a sample of changes.
CC-3 Control software libraries.	
1. Programs are labeled and inventoried.	1. Review pertinent policies and procedures. 2. Interview personnel responsible for library control. 3. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. 4. Determine how many prior versions of software modules are maintained.
2. Access to program libraries is restricted.	1. Examine libraries in use. 2. Interview library control personnel. 3. Examine libraries in use. 4. Verify that source code exists for a selection of production load modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load modules size. 5. For critical software production programs, determine whether access control software rules are clearly defined. 6. Test access to program libraries by examining security system parameters. 7. Select some program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
3. Movement of programs and data among libraries is controlled.	1. Review pertinent policies and procedures. 2. For a selection of program changes, examine related documentation to verify that: (1) procedures for authorizing movement among libraries were followed, and (2) before and after images were compared.
Systems Software	
SS-1 Limit access to systems software.	
1. Access authorizations are appropriately limited.	1. Review pertinent policies and procedures. 2. Interview management and systems personnel regarding access restrictions. 3. Observe personnel accessing systems software, such as sensitive utilities, and note the controls encountered to gain access. 4. Attempt to access the operating system and other systems software.

Control Activity	Detailed Testing
	5. Select some systems programmers and determine whether management-approved documentation supports their access to systems software.
	6. Select some application programmers and determine whether they are not authorized access.
	7. Determine the last time the access capabilities of system programmers were reviewed.
2. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Test the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtain a list of vendor-supplied software and determine if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally review the installation of systems software components and determine whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including:
	(1) Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls.
	(2) Determine whether applications interfaces have been implemented to support operating system integrity controls, including on-line transaction monitors; database software; on-line editors; on-line direct-access storage devices, on-line operating system datasets; exits related to the operating system, security, and program products; and controls over batch processing, to include security controls, scheduler controls, and access authorities.
	(3) Evaluate the controls over external access to computer resources including networks, dial-up, LAN, WAN, RJE, and the Internet.
	(4) Identify potential opportunities to adversely impact the operating system and its products through trojan horses, viruses, and other malicious actions.
	5. Obtain a list of all systems software on test and production libraries used by the entity.
	6. Verify that access control software restricts access to systems software.

Control Activity	Detailed Testing
	7. Using security software reports, determine who has access to systems software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated In the presence of the auditor.
	8. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquire as to whether disabling has occurred.
	10. Test for default presence using vendor standard IDs and passwords.
	11. Determine what terminals are set up as master consoles and what controls exist over them.
	12. Test to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
SS-2 Monitor access to and use of systems software.	
1. Policies and techniques have been implemented for using and monitoring use of system utilities.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel regarding their responsibilities.
	3. Determine whether logging occurs and what information is logged.
	4. Review logs.
	5. Using security software reports, determine who can access the logging files.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interview technical management regarding their reviews of privileged systems software and utilities usage.
	2. Review documentation supporting their reviews.
	3. Interview management and systems personnel regarding these investigations.
	4. Review documentation supporting these investigations.
	5. Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Review documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interview management and analyze their reviews concerning the use of systems software.
	8. Determine what management reviews have been conducted, and their currency, over this area.
SS-3 Control systems software changes.	
1. Systems software changes are authorized, tested, and	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel.

Control Activity	Detailed Testing
approved before implementation.	3. Review procedures for identifying and documenting systems software problems.
	4. Interview management and systems programmers.
	5. Review the causes and frequency of any recurring systems software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	6. Determine what authorizations and documentation are required prior to initiating systems software changes.
	7. Select recent systems software changes and determine whether the authorization was obtained and the change is supported by a change request document.
	8. Determine the procedures used to test and approve systems software prior to its implementation.
	9. Select recent systems software changes and test whether the indicated procedures were in fact used.
	10. Review procedures used to control and approve emergency changes.
	11. Select some emergency changes to systems software and test whether the indicated procedures were in fact used.
2. Installation of systems software is documented and reviewed.	1. Interview management and systems programmers about scheduling and giving advance notices when systems software is installed.
	2. Review recent installations and determine whether scheduling and advance notification did occur.
	3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
	4. Interview management, systems programmers, and library control personnel, and determine who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries.
	5. Review supporting documentation for some systems software migrations and the removal of outdated versions from production libraries.
	6. Interview data center management about their role in reviewing systems software installations.
	7. Review some recent systems software installations and determine whether documentation shows that logging and management review occurred.

Control Activity	Detailed Testing
	8. Interview systems software personnel concerning a selection of systems software and determine the extent to which the operating version of the systems software is currently supported by the vendor.
	9. Interview management and systems programmers about the currency of systems software and the currency and completeness of software documentation.
	10. Review documentation and test whether recent changes are incorporated.

Table D-3. Detailed MMA 912 Testing Procedures

Control Activity	Detailed Testing
Section I: Risk Assessment Review	
A. Determine if the current system configuration is documented, including links to other systems.	1. Review the most recent system configuration
	2. Review the system configuration and/or related documentation indicating it has been reviewed and kept current
B. Determine if *R*isk *A*ssessments are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.	1. Review the *R*isk *A*ssessment policies
	2. Review the most recent *R*isk *A*ssessment
	3. Review the *R*isk *A*ssessment and/or related documentation indicating it has been reviewed and conducted annually
C. Determine if data sensitivity and integrity of the data have been documented and if data has been classified	1. Review data classification policies and procedures
	2. Review evidence based on policies and procedures that data has been classified
D. Determine if threat sources, both natural and manmade, have been formally identified	1. Review *R*isk *A*ssessment to ensure that threat sources, both natural and man-made, have been identified and documented.
E. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.	1. Review the *R*isk *A*ssessment to ensure that a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed.
	2. Review the *R*isk *A*ssessment and/or related documentation indicating it has been reviewed and kept current.
F. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.	1. Review the *R*isk *A*ssessment to ensure that mitigating controls are documented.
	2. Review the *R*isk *A*ssessment to ensure that mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities.
G. Determine if final risk determinations and related management approvals have been documented and maintained on file.	1. Review the *R*isk *A*ssessment to ensure that final risk determinations are documented.
	2. Review *R*isk *A*ssessment and/or related documentation indicating it has been approved (currently).
H. Determine if a mission/business impact analysis have been conducted and documented.	1. Review documented critical business processes.
	2. Review mission/business impact analysis to ensure that it has been documented for the critical business processes
I. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Review any additional documented lists of controls identified to mitigate identified risks.
Section II: Policies and Procedures to Reduce Risk	
A. Read the policies and	1. Review the most current *R*isk *A*ssessment.

Control Activity	Detailed Testing
procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	2. Review IT Security policies and procedures to ensure that they reduce the risk outlined in the *R*isk *A*ssessment. 3. Ensure that IT Security policies and procedures are current.
B. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Review the most current System Development Life Cycle. 2. Review additional information (i.e., System Security Plan) which outline security controls included in the cost of developing new systems 3. Review software change control policies and procedures to ensure that changes are being controlled effectively.
C. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	1. Perform inquiries of appropriate personnel regarding major systems maintained at the site. 2. Review documentation indicating accreditations and certifications were performed for the noted systems. 3. Ensure that accreditations and certifications are in compliance with FISMA policies .
D. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.	1. Perform inquiries of appropriate personnel regarding systems for which controls have been tested. 2. Review evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems. 3. Review evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits. 4. Ensure that all reviews have been performed within the scope of the review.
E. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Review the most recent CMS CSR. 2. GAPs in compliance as documented in the CMS CSR. 3. Review management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
F. Determine if security policies and procedures include controls to address platform security configurations, and patch management.	1. Review platform security configuration policies and procedures. 2. Review patch management policies and procedures.
Section III: Review of System Security Plans	
A. Determine if a security plan is	1. Review most current System Security Plan.

Control Activity	Detailed Testing
documented and approved.	2. Review documentation indicating the System Security Plan was approved by appropriate individuals.
B. Determine if the plan is kept current.	1. Review previous and current System Security Plan to ensure that updates have been made as necessary.
	2. Review the date of the most current System Security Plan to ensure that it is in the scope of the review.
C. Determine if a security management structure has been established.	1. Review the security management's organizational chart.
D. Determine if information security responsibilities are clearly assigned.	1. Review the security management's organization chart.
	2. Review the security management's formal job descriptions.
E. Determine if owners and users are aware of security policies.	1. Review security training schedules.
	2. Review security training materials.
	3. For a selection of owners and users ensure that they have attended the required trainings.
F. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	1. Review the most current System Development Life Cycle.
	2. Review additional System Development Life Cycle policies and procedures to ensure that security polices and procedures have been incorporated.
	3. Perform inquiries of appropriate personnel regarding major systems maintained at the site
	4. Review documentation indicating accreditations and certifications were performed for the noted systems.
G. Determine if hiring, transfer, termination and performance policies address security.	1. Review hiring policies and procedure to ensure that they address security.
	2. Review transfer policies and procedures to ensure that they address security.
	3. Review termination policies and procedures to ensure that they address security.
	4. Review performance policies and procedures (i.e., Rules of Behavior and Performance Evaluations) to ensure they address security.
H. Determine if employee background checks are performed.	1. Review policies and procedures for performing background checks.
	2. Select a sample of employees and ensure that background investigations have been completed.
I. Determine if security employees have adequate security training and expertise.	1. Identify all employees responsible for administering security.
	2. Review training records and certifications for all security employees to ensure that adequate training has been received.

Control Activity	Detailed Testing
J. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Review policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Review documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
K. Determine if management ensures that corrective actions are effectively implemented.	1. Review policies and procedures for ensuring that corrective actions are effectively implemented.
	2. Review evidence that management ensures that corrective actions are effectively implemented.
Section IV: Review of Security Awareness Training	
A. Determine if employees have received a copy of the Rules of Behavior.	1. Inquire of the appropriate personnel regarding the maintenance and distribution of the Rules of Behavior for all types of employees.
	2. Review the most current version of the Rules of Behavior.
	3. Select a sample of employees and ensure that they have received a copy of the most current version of the rules of behavior.
B. Determine if employee training and professional development has been documented and formally monitored.	1. Inquire of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development.
	2. Review policies and procedures regarding the documentation and formal monitoring of employee training and professional development.
	3. For a selected sample of employees, review evidence that training and professional development is documented and formally monitored.
C. Determine if there is mandatory annual refresher training for security.	1. Review policies and procedures regarding mandatory annual refresher security training.
	2. Review the most recent security awareness training curriculum.
	3. For a selected sample of employees, review evidence that all attended the mandatory annual refresher security training.
D. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	1. Review policies and procedures regarding methods to make employees aware of security.
	2. Conduct a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas.
	3. Inspect evidence that methods to make employees aware of security are implemented.
E. Determine if employees have received a copy of or have easy access to agency security	1. Inquire of appropriate personnel regarding employee access to agency security procedures and policies.

Control Activity	Detailed Testing
procedures and policies.	2. Inspect evidence that employees have received a copy or have easy access to the agency security procedures and policies.
	3. Review policies and procedures in which employees have easy access to ensure that they are the most current.
F. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identify all employees responsible for administering security.
	2. Review training records and certifications for all security employees to ensure that adequate training has been received.
	3. Inquire of appropriate personnel regarding the documentation and tracking of application specific training for employees.
	4. Review the most recent application specific training curriculum.
	5. Inspect evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
Section V: Review of periodic testing and evaluation of the effectiveness of IT security policies	
A. Determine if management reports for the review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspect evidence that periodic testing of IT security policies and procedures (including network *R*isk *A*ssessments, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.
B. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspect evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
C. Determine if remedial action is being taken for issues noted on audits.	1. Review policies and procedures for taking remedial action for issues noted on audits.
	2. Inspect evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.

Control Activity	Detailed Testing
Section VI: Review of Remedial Activities, processes, and reporting for deficiencies	
A. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Review policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness.
	2. Inspect evidence that weaknesses are tracked in a formal database (or other manner).
	3. Inspect evidence that planned actions to address all IT security weaknesses is being tracked.
B. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Review policies and procedures for preparing the CAP.
	2. Review all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
C. Determine the number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Review policies and procedures for preparing CAPs.
	2. Review all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed.
	3. Inspect evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
Section VII: Review of Incident Detection, reporting, and response	
A. Determine that management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.	1. Review policies and procedures for monitoring systems and networks for unusual activity, and or intrusion attempts.
	2. Inspect evidence that management is monitoring systems and networks for unusual activity and/or intrusion attempts based on the policies and procedures.
B. Determine if management has procedures to take and has taken action in response to unusual activity, intrusion attempts and actual intrusions.	1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Inspect evidence that management has taken action in response to unusual activity, intrusion attempts, and/or actual intrusions if any have occurred within the scope of the review.
C. Determine that management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Ensure that that policies and procedures are in accordance with FISMA standards.
Section VIII: Policies and procedures for continuity of operations and related physical security safeguards for IT systems.	

Control Activity	Detailed Testing
A. Determine if critical data and operations are formally identified and prioritized.	1. Review the Business Contingency Plan to ensure that critical data and operations are formally identified and prioritized.
B. Determine if resources supporting critical operations are identified in contingency plans.	1. Review the Business Contingency Plan to ensure that resources supporting critical operations are identified.
C. Determine if emergency processing priorities are established.	1. Review emergency processing priorities to ensure that they are formally documented.
D. Determine if data and program backup procedures have been implemented.	1. Review data and program backup policies and procedures.
	2. Inspect evidence (i.e., backup logs) that data and program backup procedures have been implemented.
E. Determine if adequate environmental controls have been implemented.	1. Inquire of data center manager concerning the environmental controls implemented in the data center.
	2. Perform Walkthrough of data center to ensure that adequate environmental controls have been implemented.
F. Determine if staff have been trained to respond to emergencies.	1. Review emergency response policies and procedures.
	2. Review emergency response training curriculum.
	3. Inspect evidence that emergency response training has been provided for applicable staff.
G. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	1. Ensure that hardware maintenance procedures exist to help prevent unexpected interruptions.
	2. Ensure that problem management procedures exist to help prevent unexpected interruptions.
	3. Ensure that change management procedures exist to help prevent unexpected interruptions.
H. Determine if policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	1. Review policies and procedures regarding the disposal of data and equipment to ensure that applicable Federal security and privacy requirements are included.
I. Determine if an up-to-date contingency plan is documented.	1. Inspect evidence that the contingency plan was approved within the scope of the review.
J. Determine if arrangements have been made for alternate data processing and telecommunications facilities.	1. Review the contingency plan to ensure that arrangements have been made for alternate data processing and telecommunications facilities.
	2. Review the contract with the organization that will provide alternate data processing and telecommunications operations if necessary.

Control Activity	Detailed Testing
K. Determine if the plan is periodically tested.	1. Review policies and procedures regarding periodically testing the contingency plan.
	2. Inspect evidence that the contingency plan has been periodically tested.
L. Determine if the results are analyzed and contingency plans adjusted accordingly.	1. Inspect evidence that the contingency plan is adjusted accordingly after the tests are performed and analyzed.
M. Determine if physical security controls exist to protect IT resources.	1. Inquire of data center manager concerning the physical security controls implemented in the data center.
	2. Perform Walkthrough of data center to ensure that adequate physical security controls exist.

Table D-4. Detailed SAS 70 Testing Procedures

Control Activity	Detailed Testing
A.1 An entity-wide security program has been documented, approved and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure and clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness and ensure security officer training and employee security awareness.	
1. A security plan is documented and approved.	1. Reviewed the security plan.
	2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
2. The security plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed, updated and is current.
3. A security management structure has been established.	1. Reviewed the security plan and the entity's organization chart.
	2. Interviewed security management staff.
	3. Reviewed pertinent organization charts and job descriptions.
4. Information security responsibilities are clearly assigned.	1. Reviewed the security plan.
	2. Reviewed the security management's organization chart.
	3. Reviewed the security management's formal job descriptions.
5. Owners and users are aware of security policies.	1. Reviewed documentation supporting or evaluating the awareness program. Observed a security briefing.
	2. Interviewed data owners and system users. Determined what training they have received and if they are aware of their security-related responsibilities.
	3. Reviewed memos, electronic mail files, or other policy distribution mechanisms.
	4. Reviewed personnel files to test whether security awareness statements are current.
	5. Called selected users, identified yourself as security or network staff, and attempted to talk them into revealing their password.
	6. Reviewed security training schedules.
	7. Reviewed security training materials.
	8. For a selection of owners and users ensured that they have attended the required trainings.
6. Management periodically assesses the appropriateness of security policies and compliance with them.	1. Reviewed the reports resulting from recent assessments, including the most recent FMFIA report.
	2. Determined when last independent review or audit occurred and reviewed results.

Control Activity	Detailed Testing
	3. Reviewed written authorizations or accreditation statements.
	4. Reviewed documentation related to corrective actions.
	5. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	6. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
7. Employees have adequate training and expertise.	1. Reviewed job descriptions for security management personnel, and for a selection of other personnel.
	2. For a selection of employees, compared personnel records on education and experience with job descriptions.
	3. Reviewed training program documentation.
	4. Reviewed training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
8. Employee training and professional development has been documented and formally monitored.	1. Inquired of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development.
	2. Reviewed policies and procedures regarding the documentation and formal monitoring of employee training and professional development.
	3. For a selected sample of employees, reviewed evidence that training and professional development is documented and formally monitored.
9. There is mandatory annual refresher training for security.	1. Reviewed policies and procedures regarding mandatory annual refresher security training
	2. Reviewed the most recent security awareness training curriculum.
	3. For a selected sample of employees, reviewed evidence that all attended the mandatory annual refresher security training.
10. Systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	1. Reviewed policies and procedures regarding methods to make employees aware of security.
	2. Conducted a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas.
	3. Inspected evidence that methods to make employees aware of security are implemented.
11. Employees have received a copy of or have easy access to agency security procedures and	1. Inquired of appropriate personnel regarding employee access to agency security procedures and policies.

Control Activity	Detailed Testing
policies.	2. Inspected evidence that employees have received a copy or have easy access to the agency security procedures and policies.
	3. Reviewed policies and procedures in which employees have easy access to ensure that they are the most current.
12. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identified all employees responsible for administering security.
	2. Reviewed training records and certifications for all security employees to ensure that adequate training has been received.
	3. Inquired of appropriate personnel regarding the documentation and tracking of application specific training for employees.
	4. Reviewed the most recent application specific training curriculum.
	5. Inspected evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual and temporary) and include termination and transfer procedures that require exit interviews, return of property, such as keys and ID cards, notification to security management of terminations, removal of access to systems and escorting of terminated employees out of the facility.	
1. Hiring, transfer, termination, and performance policies address security.	1. Reviewed hiring policies and procedure to ensure that they address security.
	2. Reviewed transfer policies and procedures to ensure that they address security.
	3. Reviewed termination policies and procedures to ensure that they address security.
	4. Ensured that performance policies and procedures (i.e., Rules of Behavior and Performance Evaluations) address security.
	5. Reviewed reinvestigation policies.
	6. Reviewed policies and procedures for performing background checks.
	7. For a selection of sensitive positions, inspected personnel records and determined whether background reinvestigations have been performed.
	8. Reviewed policies on confidentiality or security agreements.
	9. For a selection of such users, determined whether confidentiality or security agreements are on file.
	10. Reviewed vacation policies.

Control Activity	Detailed Testing
	11. Inspected personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	12. Determined who performed vacationing employee's work during vacation.
	13. Reviewed job rotation policies.
	14. Reviewed staff assignment records and determined whether job and shift rotations occur.
	15. Reviewed pertinent policies and procedures.
	16. For a selection of terminated or transferred employees, examined documentation showing compliance with policies.
	17. Compared a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
3. Employees have received a copy of the Rules of Behavior.	1. Inquired of the appropriate personnel regarding the maintenance and distribution of the Rules of Behavior for all types of employees.
	2. Reviewed the most current version of the Rules of Behavior.
	3. Selected a sample of employees and ensured that they have received a copy of the most current version of the rules of behavior.
A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.	
1. Resource classifications and related criteria have been established.	1. Reviewed data classification policies and procedures.
	2. Interviewed resource owners.
2. Owners have classified resources.	1. Reviewed resource classification documentation and compared to *R*isk *A*ssessments. Discussed any discrepancies with appropriate officials.
3. Data sensitivity and integrity have been documented and data has been classified.	1. Reviewed evidence based on policies and procedures that data has been classified.
A.4 Access to computerized applications, systems software, and Medicare data is appropriately authorized, documented, and monitored, and includes approval by resource owners, procedures to control emergency and temporary access, and procedures to share and properly dispose of data.	
1. Resource owners have	1. Reviewed pertinent written policies and procedures.

Control Activity	Detailed Testing
identified authorized users and their access authorized.	2. For a selection of users (both application user and information security personnel) reviewed access authorization documentation.
	3. Interviewed owners and reviewed supporting documentation. Determined whether inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, reviewed authorization and justification.
	5. Interviewed security managers and reviewed documentation provided to them.
	6. Reviewed a selection of recent profile changes and activity logs.
	7. Obtained a list of recently terminated employees from Personnel and, for a selection, determined whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Reviewed pertinent policies and procedures.
	2. Compared a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.
	3. Determined the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examined standard approval forms.
	2. Interviewed data owners.
	3. Examined documents authorizing file sharing and file sharing agreements.
4. Sanitation of equipment and media prior to disposal or reuse.	1. Reviewed written procedures.
	2. Interviewed personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examined documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, tested that they have been appropriately sanitized.
5. Access authorizations are appropriately limited.	1. Reviewed policies and procedures regarding the disposal of data and equipment to ensure that applicable Federal security and privacy requirements are included.
	2. Interviewed management and systems personnel regarding access restrictions.
	3. Observed personnel accessing systems software, such as sensitive utilities, and noted the controls encountered to gain access.
	4. Attempted to access the operating system and other systems software.

Control Activity	Detailed Testing
	5. Selected some systems programmers and determined whether management-approved documentation supports their access to systems software.
	6. Selected some application programmers and determined whether they are not authorized access.
	7. Determined the last time the access capabilities of system programmers were reviewed.
6. Passwords, tokens, or other devices are used to identify and authenticate users.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security software password parameters.
	3. Observed users keying in passwords.
	4. Attempted to log on without a valid password; make repeated attempts to guess passwords.
	5. Assessed procedures for generating and communicating passwords to users.
	6. Reviewed a system-generated list of current passwords.
	7. Searched password file using audit software.
	8. Attempted to log on using common vendor supplied passwords.
	9. Interviewed users and security managers.
	10. Reviewed a list of IDs and passwords.
	11. Repeatedly attempted to log on using invalid passwords.
	12. Reviewed security logs.
	13. Reviewed pertinent policies and procedures.
	14. Reviewed documentation of such comparisons.
	15. Interviewed security managers.
	16. Made comparison using audit software.
	17. Viewed dump of password files (e.g., hexadecimal printout).
	18. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor obtained the assistance of a specialist.
7. Identification of access paths.	1. Reviewed access path diagram.
8. Logical controls over data files and software programs.	1. Interviewed security administrators and system users.
	2. Reviewed security software parameters.
	3. Observed terminals in use.
	4. Reviewed a system-generated list of inactive logon IDs, and determined why access for these users has not been terminated.

Control Activity	Detailed Testing
	5. Determined library names for sensitive or critical files and libraries and obtained security reports of related access rules. Using these reports, determined who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Performed penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system.
	7. When performing outsider tests, tested the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
	8. When performing insider tests, used an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, tried to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determined whether naming conventions are used.
9. Logical controls over a database.	1. Reviewed pertinent policies and procedures.
	2. Interviewed database administrator.
	3. Reviewed DBMS and DD security parameters.
	4. Tested controls by attempting to access restricted files.
	5. Reviewed security system parameters.
10. Logical controls over telecommunications access.	1. Reviewed pertinent policies and procedures.
	2. Reviewed parameters set by communications software or teleprocessing monitors.
	3. Tested telecommunications controls by attempting to access various files through communications networks.
	4. Identified all dial-up lines through automatic dialer software routines and compared with known dial-up access. Discussed discrepancies with management.
	5. Interviewed telecommunications management staff and users.
	6. Reviewed pertinent policies and procedures.
	7. Viewed the opening screen seen by telecommunication system users.
	8. Reviewed the documentation showing changes to dial-in numbers.
	9. Reviewed entity's telephone directory to verify that the numbers are not listed.

Control Activity	Detailed Testing
11. Cryptographic tools.	1. To evaluate cryptographic tools, the auditor obtained the assistance of a specialist.
A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.	
1. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Tested the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtained a list of vendor-supplied software and determined if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally reviewed the installation of systems software components and determined whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Performed an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.
	5. Obtained a list of all systems software on test and production libraries used by the entity.
	6. Verified that access control software restricts access to systems software.
	7. Using security software reports, determined who has access to systems software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated In the presence of the auditor.
	8. Verified that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquired whether disabling has occurred.
	10. Tested for default presence using vendor standard IDs and passwords.
	11. Determined what terminals are set up as master consoles and what controls exist over them.
	12. Tested to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
2. Security policies and procedures include controls to address platform security configurations, and patch management.	1. Reviewed platform security configuration policies and procedures.
	2. Reviewed patch management policies and procedures.

Control Activity	Detailed Testing
3. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
A.6 Physical access by all employees, including visitors, to Medicare facilities, data centers and systems is appropriately authorized, documented, and access violations are monitored and investigated.	
1. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Reviewed a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.
	2. Performed a walkthrough of data center to ensure that adequate physical security controls exist.
	3. Reviewed lists of individuals authorized access to sensitive areas and determined the appropriateness for access.
	4. Before becoming recognized as the auditor, attempted to access sensitive areas without escort or identification badges.
	5. Observed entries to and exits from facilities during and after normal business hours.
	6. Observed utilities access paths.
	7. Inquired of data center manager concerning the physical security controls implemented in the data center.
	8. Observed entries to and exits from sensitive areas during and after normal business hours.
	9. Reviewed procedures for the removal and return of storage media from and to the library.
	10. Selected from the log some returns and withdrawals, verified the physical existence of the tape or other media, and determined whether proper authorization was obtained for the movement.
	11. Observed practices for safeguarding keys and other devices.
	12. Reviewed written emergency procedures.
	13. Examined documentation supporting prior fire drills.
	14. Observed a fire drill.
2. Visitors are controlled.	1. Reviewed visitor entry logs.
	2. Observed entries to and exits from sensitive areas during and after normal business hours.
	3. Interviewed guards at facility entry.

Control Activity	Detailed Testing
	4. Reviewed documentation on and logs of entry code changes.
	5. Observed appointment and verification procedures for visitors.
3. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security violation reports.
	3. Examined documentation showing reviews of questionable activities.
4. Suspicious access activity is investigated and appropriate action is taken.	1. Tested a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
	2. Interviewed senior management and personnel responsible for summarizing violations.
	3. Reviewed any supporting documentation.
5. Physical security controls exist to protect IT resources.	1. Inquired of data center manager concerning the physical security controls implemented in the data center.
	2. Performed walkthrough of data center to ensure that adequate physical security controls exist.
6. Physical and logical access controls have been established.	1. Interviewed management and subordinate personnel.
A.7 Medicare application and related systems software development and maintenance activities are authorized, documented, tested, and approved.	
1. Authorizations for software modifications are documented and maintained,	1. Identified recent software modifications and determined whether change request forms were used.
	2. Examined a selection of software change request forms for approvals.
	3. Interviewed software development staff.
2. Emergency changes are promptly tested and approved.	1. Reviewed procedures.
	2. For a selection of emergency changes recorded in the emergency change log, reviewed related documentation and approval.
3. Systems software changes are authorized, tested, and approved before implementation.	1. Reviewed pertinent policies and procedures.
	2. Interviewed management and systems personnel.
	3. Reviewed procedures for identifying and documenting systems software problems.
	4. Interviewed management and systems programmers.
	5. Reviewed the causes and frequency of any recurring systems software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	6. Determined what authorizations and documentation are required prior to initiating systems software changes.

Control Activity	Detailed Testing
	7. Selected recent systems software changes and determined whether the authorization was obtained and the change is supported by a change request document.
	8. Determined the procedures used to test and approve systems software prior to its implementation.
	9. Selected recent systems software changes were tested to verify indicated procedures were in fact used.
	10. Reviewed procedures used to control and approve emergency changes.
	11. Selected some emergency changes to systems software and tested whether the indicated procedures were in fact used.
4. Installation of systems software is documented and reviewed.	1. Interviewed management and systems programmers about scheduling and giving advance notices when systems software is installed.
	2. Reviewed recent installations and determine whether scheduling and advance notification did occur.
	3. Determined whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
	4. Interviewed management, systems programmers, and library control personnel, and determined who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries.
	5. Reviewed supporting documentation for some systems software migrations and the removal of outdated versions from production libraries.
	6. Interviewed data center management about their role in reviewing systems software installations.
	7. Reviewed some recent systems software installations and determined whether documentation shows that logging and management review occurred.
	8. Interviewed systems software personnel concerning a selection of systems software and determined the extent to which the operating version of the systems software is currently supported by the vendor.
	9. Interviewed management and systems programmers about the currency of systems software and the currency and completeness of software documentation.
	10. Reviewed documentation and tested whether recent changes are incorporated.

Control Activity	Detailed Testing
5. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Reviewed the most current System Development Life Cycle. 2. Reviewed additional information (i.e., System Security Plan) which outline security controls included in the cost of developing new systems. 3. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
6. Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	1. Performed inquiries of appropriate personnel regarding major systems maintained at the site. 2. Reviewed documentation indicating accreditations and certifications were performed for the noted systems. 3. Ensured that accreditations and certifications are in compliance with FISMA policies .
A.8 A System Development Life Cycle methodology is documented and in use and includes planning for and costs for security requirements in systems.	
1. A system development life cycle methodology (SDLC) has been implemented.	1. Reviewed SDLC methodology. 2. Reviewed system documentation to verify that SDLC methodology was followed. 3. Interviewed staff. 4. Reviewed training records.
2. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Reviewed additional information (i.e., System Security Plan) which outline security controls included in the cost of developing new systems. 2. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
3. Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	1. Reviewed additional System Development Life Cycle policies and procedures to ensure that security polices and procedures have been incorporated. 2. Performed inquiries of appropriate personnel regarding major systems maintained at the site. 3. Reviewed documentation indicating accreditations and certifications were performed for the noted systems
A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.	
1. Authorizations for software modifications are documented and maintained.	1. Identified recent software modifications and determined whether change request forms were used. 2. Examined a selection of software change request forms for approvals. 3. Interviewed software development staff.

Control Activity	Detailed Testing
2. Use of public domain and personal software is restricted.	1. Reviewed pertinent policies and procedures. 2. Interviewed users and data processing staff.
3. Changes are controlled as programs progress through testing to final approval.	1. Reviewed test plan standards. 2. For the selected software change requests (1) reviewed specifications; (2) traced changes from code to design specifications; (3) reviewed test plans; (4) compared test documentation with related test plans; (5) analyzed test failures to determine if they indicate ineffective software testing; (6) reviewed test transactions and data. 3. For the software change requests selected for control activity CC-1.2 (continued): (1) reviewed test results; (2) reviewed documentation of management or security administrator reviews; (3) verified user acceptance; and (4) reviewed updated documentation. 4. Determined whether operational systems experienced a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
4. Emergency processing priorities are established.	1. Reviewed emergency processing priorities to ensure that they are formally documented.
5. Data and program backup procedures have been implemented.	1. Reviewed data and program backup policies and procedures. 2. Inspected evidence (i.e., backup logs) that data and program backup procedures have been implemented.
6. Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	1. Reviewed hardware maintenance procedures that exist to help prevent unexpected interruptions. 2. Reviewed problem management procedures that exist to help prevent unexpected interruptions. 3. Reviewed change management procedures that exist to help prevent unexpected interruptions.
A.10 Access to program libraries is properly restricted and movement of programs among libraries is controlled.	
1. Programs are labeled and inventoried.	1. Reviewed pertinent policies and procedures. 2. Interviewed personnel responsible for library control. 3. Examined a selection of programs maintained in the library and assessed compliance with prescribed procedures. 4. Determined how many prior versions of software modules are maintained.
2. Access to program libraries is restricted.	1. Examined libraries in use. 2. Interviewed library control personnel. 3. Verified that source code exists for a selection of production load modules.

Control Activity	Detailed Testing
	4. For critical software production programs, determined whether access control software rules are clearly defined.
	5. Tested access to program libraries by examining security system parameters.
	6. Selected some program tapes from the log and verified the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
3. Movement of programs and data among libraries is controlled.	1. Reviewed pertinent policies and procedures.
	2. For a selection of program changes, examined related documentation to verify that: (1) procedures for authorizing movement among libraries were followed, and (2) before and after images were compared.
A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.	
1. Incompatible duties have been identified and policies implemented to segregate these duties.	1. Reviewed pertinent policies and procedures.
	2. Interviewed selected management and information security personnel regarding segregation of duties.
	3. Reviewed an agency organization chart showing information security functions and assigned personnel.
	4. Interviewed selected personnel and determined whether functions are appropriately segregated.
	5. Determined whether the chart is current and each function is staffed by different individuals.
	6. Reviewed relevant alternate or backup assignments and determined whether the proper segregation of duties is maintained.
	7. Observed activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	8. Reviewed the organizational chart and interviewed personnel to determine that assignments do not result in a single person being responsible for the indicated combination of functions.
	9. Determined through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	10. Reviewed the adequacy of documented operating procedures for the data center.
2. Job descriptions have been documented.	1. Reviewed job descriptions for several positions in organizational units and for user security administrators.
	2. Determined whether duties are clearly described and prohibited activities are addressed.

Control Activity	Detailed Testing
	3. Reviewed the effective dates of the position descriptions and determined whether they are current.
	4. Compared these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	5. Reviewed job descriptions and interviewed management personnel.
3. Employees understand their duties and responsibilities.	1. Interviewed personnel filling positions for the selected job descriptions (see above). Determined if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	2. Determined from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	3. Interviewed management personnel in these activities.
4. Management reviews effectiveness of control techniques.	1. Interviewed management and subordinate personnel.
	2. Selected documents or actions that require supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	3. Determined which reviews are conducted to assess the adequacy of duty segregation. Obtained and reviewed results of such reviews.
5. Formal procedures guide personnel in performing their duties.	1. Reviewed manuals.
	2. Interviewed supervisors and personnel.
	3. Observed processing activities.
6. Active supervision and review are provided for all personnel.	1. Interviewed supervisors and personnel.
	2. Observed processing activities.
	3. Reviewed history log reports for signatures indicating supervisory review.
	4. Determined who is authorized to perform the initial program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determined whether operators override the IPL parameters.
A.12 Activities of employees should be controlled via formal operating procedures that include monitoring of employee activities by management with documentation maintained to provide evidence of management's monitoring and review process.	
1. Audit trails are maintained.	1. Reviewed security software settings to identify

Control Activity	Detailed Testing
	types of activity logged.
2. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security violation reports.
	3. Examined documentation showing reviews of questionable activities.
3. Policies and techniques have been implemented for using and monitoring use of system utilities.	1. Reviewed pertinent policies and procedures.
	2. Interviewed management and systems personnel regarding their responsibilities.
	3. Determined whether logging occurs and what information is logged.
	4. Reviewed logs.
	5. Using security software reports, determined who can access the logging files.
4. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interviewed technical management regarding their reviews of privileged systems software and utilities usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel regarding these investigations.
	4. Reviewed documentation supporting these investigations.
	5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interviewed management and analyzed their reviews concerning the use of systems software.
	8. Determined what management reviews have been conducted, and their currency, over this area.
5. Formal procedures guide personnel in performing their duties.	1. Reviewed manuals.
	2. Interviewed supervisors and personnel.
	3. Observed processing activities.
6. Active supervision and review are provided for all personnel.	1. Interviewed supervisors and personnel.
	2. Observed processing activities.
	3. Reviewed history log reports for signatures indicating supervisory review.
A.13 A regular *R*isk *A*ssessment of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.	
1. Risks are periodically assessed.	1. Reviewed *R*isk *A*ssessment policies.
	2. Reviewed the most recent high-level *R*isk *A*ssessment.

Control Activity	Detailed Testing
	3. Reviewed the objectivity of personnel who performed and reviewed the assessment.
2. The current system configuration is documented, including links to other systems.	1. Reviewed the most recent system configuration.
	2. Reviewed the system configuration and/or related documentation indicating it has been reviewed and kept current.
3. Data sensitivity and integrity of the data have been documented and if data have been classified.	1. Reviewed data classification policies and procedures
	2. Reviewed evidence based on policies and procedures that data have been classified
4. Threat sources, both natural and manmade, have been formally identified.	1. Reviewed *R*isk *A*ssessment to ensure that threat sources, both natural and man-made, have been identified and documented.
5. A list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.	1. Reviewed the *R*isk *A*ssessment to ensure that a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed.
	2. Reviewed the *R*isk *A*ssessment and/or related documentation indicating it has been reviewed and kept current.
6. An analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.	1. Reviewed the *R*isk *A*ssessment to ensure that mitigating controls are documented.
	2. Reviewed the *R*isk *A*ssessment to ensure that mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities.
7. Final risk determinations and related management approvals have been documented and maintained on file.	1. Reviewed the *R*isk *A*ssessment to ensure that final risk determinations are documented.
	2. Reviewed *R*isk *A*ssessment and/or related documentation indicating it has been approved (currently).
8. A mission/business impact analysis have been conducted and documented.	1. Reviewed documented critical business processes.
	2. Reviewed mission/business impact analysis to ensure that it has been documented for the critical business processes.
9. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
10. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic	1. Performed inquiries of appropriate personnel regarding systems for which controls have been tested.
	2. Reviewed evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems.

Control Activity	Detailed Testing
reviews/audits.	3. Reviewed evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits.
	4. Ensured that all reviews have been performed within the scope of the review.
A.14 A centralized risk management focal point for IT *R*isk *A*ssessment has been established that includes promotion awareness programs, processes and procedures to mitigate risks, and monitoring processes to assess the effectiveness of risk mitigation programs.	
1. A security management structure has been established.	1. Reviewed the security plan and the entity's organization chart.
	2. Interviewed security management staff.
	3. Reviewed pertinent organization charts and job descriptions.
	4. Interviewed the security manager.
2. Information security responsibilities are clearly assigned.	1. Reviewed the security plan.
3. Final risk determinations and related management approvals have been documented and maintained on file.	1. Reviewed the *R*isk *A*ssessment to ensure that final risk determinations are documented.
	2. Reviewed *R*isk *A*ssessment and/or related documentation indicating it has been approved (currently).
4. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
5. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	1. Reviewed the most current *R*isk *A*ssessment.
	2. Reviewed IT Security policies and procedures to ensure that they reduce the risk outlined in the *R*isk *A*ssessment.
	3. Ensured that IT Security policies and procedures are current.
6. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
7. Management reports for the review and testing of IT security policies and procedures, including network *R*isk *A*ssessment, accreditations	1. Inspected evidence that periodic testing of IT security policies and procedures (including network *R*isk *A*ssessments, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have

Control Activity	Detailed Testing
and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	been conducted.
8. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
A.15 A Risk Assessment and System Security Plan has been documented, approved, and monitored by management in accordance with the CMS Risk Assessment and System Security Plan Methodologies.	
1. Risks are periodically assessed.	1. Reviewed *R*isk *A*ssessment policies.
	2. Reviewed the most recent high-level *R*isk *A*ssessment.
	3. Reviewed the objectivity of personnel who performed and reviewed the assessment.
2. A security plan is documented and approved.	1. Reviewed the security plan.
	2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
3. The plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed and updated and is current.
A.16 Regularly scheduled processes required to support the Medicare contractor's continuity of operations (data, facilities or equipment) are performed.	
1. Data and program backup procedures have been implemented.	1. Reviewed written policies and procedures for backing up files.
	2. Compared inventory records with the files maintained off-site and determined the age of these files.
	3. For a selection of critical files, located and examined the backup files. Verified that backup files can be used to recreate current reports.
	4. Determined whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	5. Located and examined documentation.
	6. Examined the backup storage site.
2. Adequate environmental controls have been	1. Examined the entity's facilities
	2. Interviewed site managers.

Control Activity	Detailed Testing
implemented.	3. Observed that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observed the operation, location, maintenance and access to the air cooling system.
	5. Observed whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determined whether the activation of heat and smoke detectors will notify the fire department.
3. Staff have been trained to respond to emergencies.	1. Interviewed data center staff.
	2. Reviewed training records.
	3. Reviewed training course documentation.
	4. Reviewed emergency response procedures.
	5. Reviewed test policies.
	6. Reviewed test documentation.
	7. Interviewed data center staff.
4. Effective hardware maintenance, problem management, and change management procedures exist.	1. Reviewed hardware maintenance procedures.
	2. Reviewed problem management procedures.
	3. Reviewed change management procedures.
A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components and operations.	
1. Management ensures that corrective actions are effectively implemented.	1. Reviewed the status of prior-year audit recommendations and determined if implemented corrective actions have been tested.
	2. Reviewed recent FMFIA reports.
	3. Reviewed policies and procedures for ensuring that corrective actions are effectively implemented.
	4. Reviewed evidence that management ensures that corrective actions are effectively implemented.
2. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Reviewed the most recent CMS CSR.
	2. Noted GAPs in compliance as documented in the CMS CSR.
	3. Reviewed management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
3. Weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Reviewed policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness.
	2. Inspected evidence that weaknesses are tracked in a formal database (or other manner).

Control Activity	Detailed Testing
	3. Inspected evidence that planned actions to address all IT security weaknesses are being tracked.
4. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Reviewed policies and procedures for preparing CAPs.
	2. Reviewed all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
5. The number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Reviewed policies and procedures for preparing CAPs.
	2. Reviewed all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed.
	3. Inspected evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
6. Remedial action is being taken for issues noted on audits.	1. Reviewed policies and procedures for taking remedial action for issues noted on audits.
	2. Inspected evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.
A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.	
1. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.
	2. Review documentation supporting incident handling activities.
	3. Determine qualifications of response team members.
2. Audit trails are maintained.	1. Review security software settings to identify types of activity logged.
A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts, and actual intrusions.	
1. Suspicious access activity is investigated and appropriate action is taken.	1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Tested a selection of security violations to verify that follow-up investigations were performed, and to determine what actions were taken against the perpetrator.
	3. Interviewed senior management and personnel responsible for summarizing violations.
	4. Reviewed any supporting documentation.
	5. Reviewed policies and procedures and interviewed appropriate personnel.

Control Activity	Detailed Testing
	6. Reviewed any supporting documentation.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interviewed technical management regarding their reviews of privileged systems software and utilities usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel regarding these investigations.
	4. Reviewed documentation supporting these investigations.
	5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interviewed management and analyzed their reviews concerning the use of systems software.
	8. Determined what management reviews have been conducted, and their currency, over this area.
A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the Federal Information Security Management Act (FISMA)	
1. Management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Ensured that policies and procedures are in accordance with FISMA standards.

Appendix E: ***CMS Guidelines***

CMS Guidelines

Table of Contents

1.0 Introductory Comments to CMS Guidelines on Information Technology Controls

(Rev.)

1.1 Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This document provides introductory comments for a series of guidelines issued by the Centers for Medicare and Medicaid Services (CMS) to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment. The guidelines issued consist of the following:

1) *Logical access controls and segregation of duties*

2) *Development and implementation of an entity-wide security plan*

3) *Application programmers' access to application data and source code and application programmer segregation of duties*

4) *Change management procedures and requirements for maintaining change management documentation*

5) *Testing process for the SANS Top 20 Security Weaknesses*

6) *Implementation of security configuration templates*

The intended audience of these guidelines, however, extends beyond CMS management and staff to include all CMS business partners.

Today's highly technology-dependent organization, while benefiting from the increased capabilities offered by continued improvements in Information Technology (IT), is also faced with the challenge of maintaining sufficient controls around the increased complexities of new developments in IT. The primary objectives of these controls are to maintain confidentiality, integrity, and availability around information critical to the organization's mission.

The six guidelines mentioned above will provide CMS management and business partners with the information required to ensure that key Federal government recommended controls pertaining to each of the six topics are fully incorporated into CMS' current controls management environment.

1.2 Compliance Criteria

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The IT Controls discussed in the guidelines are part of the foundation of operating in a secure environment promoting effective controls around data confidentiality, integrity, and availability. The importance of these controls is evidenced by the direct inclusion or indirect references to these controls in numerous Federal government Acts, standards, and guidelines, including, but not limited to, the following:

- *Chief Financial Officers Act of 1990*
- *Federal Financial Management Improvement Act (FFMIA) of 1996*
- *Federal Manager's Financial Integrity Act of 1982*
- *Federal Information Security Management Act of 2002 (FISMA)*
- *Various OMB circulars including OMB A-127 (Financial Management Systems) and OMB A-130 (Security of Federal Automated Information Resources)*
- *Various NIST Special Publications in the 800-series reports, and*
- *GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM)*

The guidelines focus on the identification and description of controls pertaining to each of the six control areas as recommended by FISCAM and FISMA (and other Federal government or industry standards, as required). Listed below is a brief discussion of the compliance framework for FISCAM and FISMA:

- *A key goal of the Chief Financial Officers Act of 1990 was the development of a consistent approach to financial statement audits of Federal government agencies. General Accounting Office (GAO) Financial Audit Manual (FAM) provides detailed guidance on the performance of financial statement audits. In January of 1999, GAO issued the Federal Information Systems Controls Audit Manual (FISCAM) as a companion to FAM. FISCAM provides the methodology for IT controls review within the framework of a financial statement audit of Federal government agencies.*
- *In February 2005, NIST published Special Publication (SP) 800-53 to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002. According to the OMB memorandum titled "Memorandum for Heads of Executive Departments and Agencies", dated June 13, 2005, the approach documented in NIST SP 800-53 is to be used by agencies to conduct self assessments in compliance with FISMA. The memorandum does note that the older NIST guidance (NIST SP 800-26) may also be used. For the purposes of this guideline we follow NIST SP 800-53 as the latest guidance on FISMA compliance.*

The six control areas discussed in the guidelines have manifested themselves within the management practices of CMS through the inclusion of a number of controls related to these areas in CMS' Business Partners Systems Security Manual (BPSSM). CMS has used OMB circulars, NIST Special Publication 800-series reports, and other Federal and industry guidelines to compile the IT management practices documented in BPSSM. Included in these

practices are specific measures for the implementation of core security requirements. All controls listed in the BPSSM are mandatory for all business partners of CMS. As such the content of the BPSSM are not to be viewed as "guidance'. They are, rather, "requirements" for all CMS business partners.

1.3 Organizational Approach to Controls Implementation

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

1.3.1 Year-round Cyclical Approach

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Controls which are enforced through a periodic assessment against a static controls checklist will inevitably fail. Both the operations environment and the IT environment which supports it are fluid as are the security controls required to ensure data confidentiality, integrity, and availability. As such, the implementation of any control at CMS can only be effective if it is an integral part of the management process. This means incorporation of security controls in the year-round enterprise-wide management lifecycle of the organization.

FISCAM and NIST 800-53 have each defined specific roles and responsibilities and an approach to planning and management of effective IT systems security. Within sections two (2) and three (3) of the BPSSM, CMS has also documented detailed descriptions of system security roles and responsibilities and an approach to managing IT systems security.

CMS management is committed to ensuring that:

- *Sections two (2) and three (3) of the BPSSM are continually evaluated against the IT security management approach and roles and responsibilities listed in FISCAM and NIST SP 800-53 to facilitate full compliance with these standards; and*

- *The BPSSM is continually evaluated for compliance with guidance in FISCAM and NIST SP 800-53 regarding specific systems to be covered by the security management program.*

Table E-1 maps the key components of the IT security management approach recommended by FISCAM to those recommended by NIST 800-53 and those required by BPSSM.

1.3.2 Management Involvement

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

As mentioned in the prior section, effective implementation of IT security controls can only be achieved if it is incorporated in the year-round enterprise-wide management lifecycle at the highest levels of an organization. This requires direct involvement, not only by the IT

management structure (e.g., Chief Technology Officer and Chief Information Security Officer) but also by executives at the enterprise-wide level (e.g., program managers and agency leadership). This requirement is not only reflected in the compliance criteria used for the guidelines (e.g., the reporting requirements for FISMA) but also in other IT-related government publications and standards (e.g., the revised OMB Circular A-123, effective FY 2006).

Table E-1. Mapping of IT Security Program Management Principles

FISCAM	NIST 800-53	BPSSM (includes Chapter #)
Assess Risks & Determine Needs	Periodic risk assessments	3.10 Management Security Resources 3.2 Risk Assessment
Implement Policies and Controls	System security plans Policies and procedures based (on the risk assessments) and subordinate plans for providing adequate system security Plans and Procedures to Ensure Continuity of Operations for IT Systems	3.1 System Security Plan 3.4 IT Systems Contingency Plan 3.8 Fraud Control 3.9 Patch Management
Promote Awareness	Security awareness training	Attachment A Core Set of Security Requirements
Monitor & Evaluate Policy and Control Effectiveness	Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including: Network assessments Penetration activities Change management procedures Other Remedial activities, processes and reporting for deficiencies Incident detection, reporting, and response	3.3 Certification 3.5.1 Annual Compliance Audit 3.5.2 Plan of Action and Milestones 3.6 Incident Reporting and Response 3.7 System Security Profile

1.3.3 Reporting Requirements

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Given the fact that FISCAM's intended audience is financial statement auditors (i.e., Inspector Generals and independent auditors) it contains no reporting requirements directed specifically at agency management. FISMA however contains specific reporting requirements for agency management as well as the Inspector General.

According to the OMB Memorandum for Heads of Executive Departments and Agencies, published on June 13, 2005, regarding FISMA reporting instructions, "all agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget and Congress on the effectiveness of their security programs". According to the memorandum, each agency head's annual report should be submitted to the Director of OMB and should comprise:

- *A transmittal letter from the agency head, including a discussion of any differences between the findings of the agency CIO and IG*

- *Results of annual IT security reviews of systems and programs [completed by the CIO]*

- *Results of the IG's independent evaluation [completed by the IG]*

- *Status of agency compliance with OMB privacy policies [completed by the senior agency official for privacy]*

The memorandum states that, prior to submission of the report, the CIO and IG assessment results need to be reconciled to resolve discrepancies, if any, between the two sections. It is also expected that a Plan of Action and Milestones (POA&M) will be developed by each agency to correct weaknesses identified in the above reporting process. Reports documenting FISMA compliance updates must be sent by the agency to OMB on a quarterly basis.

The memorandum emphasizes the fact that FISMA applies to information systems used or operated by an agency or by a contractor of the agency or other organization on behalf of the agency. It also states that agencies should report both at an agency-wide level as well as by individual component. Clearly, the FISMA requirements apply to CMS Business Partners listed in the Introduction

In the CMS controls environment, the BPSSM discusses a tool to help CMS business partners conduct systems security self-assessments. It is known as the Contractor Assessment Security Tool (CAST) which is a module in the CMS Integrated Security Suite (CISS) tool. This module assists business partners to prepare for periodic audits. Upon completion of a self assessment, the business partner is required to submit the database to the CMS Central Office, the Consortium Contractor Management Officer and/or CMS Project Officer (CCMO/PO) for review [along with other required security documentation which is described in section three (3) of the BPSSM]. For CMS business partners, Joint Signature Memorandum JSM-05352, dated 05-17-05, specifies that POA&M reporting is to be performed on a monthly basis.

It is critical that the security review and reporting cycle prescribed by BPSSM follow a time table that allows for timely input to the FISMA reporting process and deadlines mentioned above.

1.4 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The primary objectives of effective IT controls are to maintain confidentiality, integrity, and availability around information critical to the organization's mission. Through the implementation of effective IT Controls security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud. The implementation of the controls discussed in the six guidelines, however, should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

2.0 CMS Guidelines on Logical Access Controls and Segregation of Duties

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

2.1 Overview

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is ***logical access controls and segregation of duties****. This guideline will:*

- *Provide a high level understanding of* ***logical access controls and segregation of duties****,*
- *Facilitate the identification of IT controls, in key Federal guidelines and standards, which are directly related to* ***logical access controls and segregation of duties****, and*
- *Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.*

2.2 Introduction to Logical Access Controls and Segregation of Duties

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Business Partners Systems Security Manual (BPSSM) defines access controls as controls that "provide reasonable assurance that information handling resources are protected against unauthorized loss, modification, disclosure, and damage. Access controls can be logical or physical."

According to General Accounting Office' (GAO) Federal Information Systems Controls Audit Manual (FISCAM), key objectives of logical access controls are to ensure that (1) users have only the access needed to perform their duties, (2) access to very sensitive resources, such as security software programs, is limited to very few individuals, and (3) employees are restricted from performing incompatible functions or functions beyond their responsibility.

FISCAM states that "If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with the practical needs of users. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users."

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges. Controls should be designed to restrict legitimate users to the specific systems, programs, and files needed to perform their duties while inhibiting access by others.

FISCAM defines 'Segregation of duties' as controls that describe how work responsibilities should be segregated so that one person does not have access to or control over all of the critical stages of an information handling process. For instance; while representatives of the user community may initiate requests for changes to system capabilities, computer programmers should not be allowed to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more organizational groups to ensure independence and objective checks and balances. Controls can be enforced through automated and/or manual measures.

2.3 Risks of Non-compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Per FISCAM, "inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure and modification of data". Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- *By obtaining direct access to **data files**, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) inadvertently or purposefully change a receivable balance, or (4) obtain confidential information about business transactions or individuals.*

- *By obtaining access to **application programs** used to process transactions, an individual could make unauthorized changes to these programs or introduce malicious programs, which in turn could be used to access data files, resulting in situations similar to those describe above, or to process unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for himself or herself.*

- *By obtaining access to **computer facilities and equipment**, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.*

FISCAM states that "inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed." FISCAM provides the following examples of potential consequences of inadequate controls around segregation of duties;

- *an individual who was independently responsible for authorizing processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or*

- *a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.*

Within appendix C of the BPSSM, the Centers for Medicare and Medicaid Services (CMS) outlines a number of specific safeguards against employee fraud. ***Segregation of duties*** *is listed as a key safeguard against employee fraud. For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix C of the BPSSM.*

2.4 Specific Controls to be Implemented

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All controls documented in the BPSSM are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, ***unless other compensatory controls are in place which satisfy the control objective.***

Table E-3 and Table E-4 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to ***logical access controls and segregation of duties****. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-3. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-4.*

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare claims processing systems and Medicare data center systems be categorized as "high impact" security systems.

As mentioned above, Table E-4 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to ***logical access controls and segregation of duties****. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.*

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-4 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-4, the corresponding FISCAM control in Table E-3, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with ***logical access controls and segregation of duties*** *guidelines.*

2.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Table E-2 below provides a listing of sample instances of non-compliance with logical access controls and segregation of duties based on prior controls reviews and audits. Specifically, the table lists the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue takes into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.

Table E-2. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	*Issue*	*Suggested Remediation*
Password management controls need to be strengthened	*1. Some user accounts were not set to force the use of a combination of alphabetical, numeric, and/or special characters.*	*Force RACF password configuration settings to include a combination of alphabetical, numeric, and/or special characters (may require an exit).*

Finding	Issue	Suggested Remediation
	2. Management does not have a process for periodically reviewing user ID profiles to ensure that these profiles are not configured with inappropriate settings.	Periodically review user accounts and passwords to ensure that they adhere to BPSSM requirements and applicable FISCAM Controls and Control Techniques, e.g., access settings reflect job responsibilities, use of alpha-numeric passwords, etc. These controls can be enforced through, manual as well as automated, means.
Logical access controls need to be strengthened	1. Revoked RACF user IDs are not being promptly removed from the mainframe system.	Clarify and document the programs, processes, and procedures used to periodically review and remove "revoked" user IDs from the system. Document and maintain justifications for revoked RACF user IDs on the system, as well as, authorizations for the reactivation or deletion of these accounts.
	2. Access to the DB2 system, which contains sensitive Medicare information, is not being restricted to users on a "need to know" basis.	Update the database administration policies and procedures to include comprehensive processes and procedures regarding the maintenance of documented RACF user authorizations to access DB2 data sets containing sensitive Medicare data. Document and maintain authorizations for all RACF user IDs with access to DB2 data sets containing sensitive Medicare data. Develop, document, and implement processes and procedures to monitor user accesses to sensitive Medicare data maintained in DB2 data sets and to take appropriate action when questionable access is detected.
Resource owners have not identified or granted access to authorized users.	1. No user access documentation exists for network devices, including the Cisco router and the Cisco PIX firewall.	Continue efforts in developing a logging and monitoring strategy for Cisco routers and Cisco PIX firewalls. The strategy should be implemented on the Medicare systems and throughout the organization. A policy should also be developed to outline roles and responsibilities in ensuring that the systems are configured correctly and that logs are being generated and reviewed. A formal user access policy should be complied with for granting users access to all network devices including Cisco routers and Cisco PIX firewalls.
	2. Access to the Cisco routers and the Cisco PIX firewall are not proactively monitored.	
	3. Logging is disabled on the Cisco PIX firewall.	

Finding	Issue	Suggested Remediation
Oracle database control deficiencies	*1. A process for establishing the accounts is not defined and documented.*	*Develop and document procedures for establishing Oracle accounts.*
	2. The defined privileges are not periodically assessed and revalidated.	*Develop and document procedures for reviewing Oracle accounts, account privileges, and user roles.*
	3. Procedures for assigning user roles have not been documented.	*Develop and document procedures for assigning user roles.*
	4. Oracle logs are not reviewed and automated tools to assist in log reviews do not exist.	*Develop and document procedures for reviewing Oracle logs. Research and implement automated tools to assist in log reviews and monitoring.*
	5. The configuration setting to provide log actions performed by privileged accounts was not set.	*Configure the Oracle initialization file to generate audit logs of actions performed by privileged users.*
Improvements in Password controls over network devices that allow Dial-in access	*1. Noted poor password controls for devices that allow access to the network. As a result, passwords could be easily guessed.*	*Management should establish, implement, and enforce formal policies and procedures for remote access password-use ensuring that "hard-to-guess" passwords are required for authentication of remote users.*
Password Parameters did not meet CMS Core Security Requirements	*For the mainframe, the following ACF2 password settings were used:*	*ACF2 policies should be improved to meet the minimum requirements outlined in the CMS Core Security Requirements. Correct and resubmit CMS CAST worksheets to reflect the current environment.*
	1. PSWD HISTORY = NO - Activates default history of one generation. Old passwords may be used after one generation	
	2. MIN PSWD LENGTH = 5 - Allowed five characters for a minimum.	

Finding	Issue	Suggested Remediation
	3. LOGON RETRY COUNT = 3 - Does not deactivate the user ID after three failed passwords, but rather logs the terminal session off. The user can immediately restart the session and conduct additional logon attempts.	
	4. MAX PSWD ATTEMPTS = 6 - Allows a user ID to have six invalid password attempts during a password change period, at which time the account is locked out.	
Job rotation and vacation policy does not exist	A formal policy mandating periodic job rotations and vacation for personnel does not exist.	We recommend that management incorporate a formal job rotation and vacation policy so that responsibilities can be re-assigned to different individuals. Should neither of the above two measures exist, we recommend the monitoring of employee activities who are exposed to sensitive data over extended periods in order to reduce potential security risks.

2.6 Periodic Review and Testing of Controls

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems, and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of

existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

2.7 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Logical access controls are controls that provide reasonable assurance that information handling resources are protected against unauthorized loss, modification, disclosure, and damage. Segregation of duties controls are controls that facilitate the separation of work responsibilities such that one person does not have access to or control over all of the critical stages of an information handling process such that unauthorized data access and modification is not prevented or detected.

*Through the implementation of effective **logical access controls and segregation of duties**, security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud.*

The implementation of these controls should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table E-3. Applicable FISCAM Controls

FISCAM General Controls
SP-1 Periodically Assess Risks
AC-1 Classify information resources according to their criticality and sensitivity
AC-1.1 Resource classifications and related criteria have been established

FISCAM General Controls
AC-1.2 Owners have classified resources
AC-2 Maintain a current list of authorized users and their access authorized
AC-2.1 Resource owners have identified authorized users and their access authorized
AC-2.2 Emergency and temporary access authorization is controlled
AC-2.3 Owners determine disposition and sharing of data
AC-3 Establish physical and logical controls to prevent or detect unauthorized access
AC-3.2 Adequate logical access controls have been implemented
A. Passwords, tokens, or other devices are used to identify and authenticate users
B. Identification of access paths
C. Logical controls over data files and software programs
D. Logical controls over a database
E. Logical controls over telecommunications access
AC-3.3 Cryptographic tools
AC-3.4 Sanitation of equipment and media prior to disposal or reuse
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action
AC-4.1 Audit trails are maintained
AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored
AC-4.3 Suspicious access activity is investigated and appropriate action taken
CC-3 Control software libraries
CC-3.2 Access to program libraries is restricted
SS-1 Limit access to system software
SS-1.1 Access authorizations are appropriately limited
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths
SS-2 Monitor access to and use of system software
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities
SD-1 Segregate incompatible duties and establish related policies
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties
SD-1.2 Job descriptions have been documented
SD-1.3 Employees understand their duties and responsibilities
SD-2 Establish access controls to enforce segregation of duties
SD-2.1 Physical and logical access controls have been established
SD-2.2 Management reviews effectiveness of control techniques
SD-3 Control personnel activities through formal operating procedures and supervision and review
SD-3.1 Formal procedures guide personnel in performing their duties
SD-3.2 Active supervision and review are provided for all personnel

Table E-4. Applicable NIST SP 800-53 Controls

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
	Family: Access Control	
	AC-1	*Access Control Policy and Procedures*
AC-2.1, AC-2.2, AC-3.2, SP-4.1	*AC-2*	*Account Management*
AC-2, AC-3.2	*AC-3*	*Access Enforcement*
	AC-4	*Information Flow Enforcement*
AC-3.2, SD-1.2	*AC-5*	*Separation of Duties*
AC-3.2	*AC-6*	*Least Privilege*
AC-3.2	*AC-7*	*Unsuccessful Login Attempts*
AC-3.2	*AC-8*	*System Use Notification*
AC-3.2	*AC-9*	*Previous Logon Notification*
	AC-10	*Concurrent Session Control*
AC-3.2	*AC-11*	*Session Lock*
AC-3.2	*AC-12*	*Session Termination*
AC-4, AC-4.3, SS-2.2	*AC-13*	*Supervision and Review -- Access Control*
	AC-14	*Permitted Actions without Identification or Authentication*
AC-3.2	*AC-15*	*Automated Marking*
AC-3.2	*AC-16*	*Automated Labeling*
AC-3.2	*AC-17*	*Remote Access*
	AC-18	*Wireless Access Restrictions*
	AC-19	*Access Control for Portable and Mobile Devices*
	AC-20	*Personally Owned Information Systems*
	Family: Awareness and Training	
	AT-1	*Security Awareness and Training Policy and Procedures*
	AT-2	*Security Awareness*
	Family: Audit and Accountability	
AC-4.3	*AU-6*	*Audit Monitoring, Analysis, and Reporting*
	Family: Identification and Authentication	
	IA-1	*Identification and Authentication Policy and Procedures*
	IA-2	*User Identification and Authentication*
	IA-3	*Device Identification and Authentication*
AC-2.1, AC-3.2, SP-4.1	*IA-4*	*Identifier Management*
AC-3.2	*IA-5*	*Authenticator Management*
	IA-6	*Authenticator Feedback*
	IA-7	*Cryptographic Module Authentication*
	Family: Personnel Security	
	PS-1	*Personnel Security Policy and Procedures*

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
SD-1.2	*PS-2*	*Position Categorization*
SP-4.1	*PS-3*	*Personnel Screening*
SP-4.1	*PS-4*	*Personnel Termination*
SP-4.1	*PS-5*	*Personnel Transfer*
SP-4.1	*PS-6*	*Access Agreements*
SP-4.1	*PS-7*	*Third-Party Personnel Security*
	PS-8	*Personnel Sanctions*
	Family: System and Information Integrity	
SD-1	*SI-9*	*Information Input Restrictions*

3.0 CMS Guidelines on Development and Implementation of an Entity-wide Security Plan

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

3.1 Overview

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is the ***development and implementation of an entity-wide security plan.*** *This guideline will:*

- *Provide a high level understanding of the* ***development and implementation of an entity-wide security plan,***
- *Facilitate the identification of IT controls, in key Federal guidelines and standards, which are directly related to the* ***development and implementation of an entity-wide security plan,*** *and*
- *Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.*

3.2 Introduction to the Development and Implementation of an Entity-wide Security Plan

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Business Partners Systems Security Manual (BPSSM) defines entity-wide security plan controls as controls that "address the planning and management of an entity's control structure."

According to General Accounting Office' (GAO) Federal Information Systems Controls Audit Manual (FISCAM), key objectives of entity-wide security program planning and management are to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer related controls.

FISCAM states that "An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."

Comprehensive guidance on planning and managing an entity-wide security plan is contained in FISCAM Appendix VIII, titled "Principles for managing an information security program."

3.3 Risks of Non-compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

In discussing security program planning and management, FISCAM states that "without a well designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources."

Within appendix C of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. Included in these safeguards are a number of security-planning related topics such as "screening new employees" and "training". For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix C of the BPSSM.

3.4 Specific Controls to be Implemented

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All controls documented in the BPSSM are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, ***unless other compensatory controls are in place, which satisfy the control objective.***

Tables E-3 and E-4 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to the ***development and implementation of an entity-wide security plan****. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-3. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-4.*

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-4 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to the development and implementation of an entity-wide security plan. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-7 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-7, the corresponding FISCAM control in Table E-6, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines around the ***development and implementation of an entity-wide security plan.***

3.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Table E-5 below provides a listing of sample instances of non-compliance with ***development and implementation of an entity-wide security plan*** *based on prior and on-going controls reviews and audits. Specifically, the table lists the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in this table are not exhaustive in that they do not list ALL current and prior instances of non-compliance at all CMS sites. A sample of prior (and on–going) audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue takes into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.*

Table E-5. Sample Findings from CMS Controls Reviews and Audits

Finding	*Issue*	*Suggested Remediation*
Data classification policy has not been fully implemented	*During our review of the data classification policy, we found that the policy has not been fully implemented.*	*The data classification policy should be fully implemented to ensure that all parties who handle data resources are aware of the security protection required for the resources.*

Finding	Issue	Suggested Remediation
Failed to conduct periodic background reinvestigations of personnel in sensitive positions	*This finding is critical not only for employees who currently hold positions categorized as highly sensitive, but also for employees who may transfer from positions requiring minimal background checks to those positions requiring higher-level security checks.*	*The Business partner should engage in active communication with CMS during the development and implementation of CMS' high-level security policy to become familiar with the required reinvestigation guidelines. CMS should implement its high-level security policy to address the requirements for periodic background reinvestigations. These requirements should ensure that positions are classified by sensitivity level and that reinvestigations are conducted for employees in all sensitive positions defined within the organization, as well as for those employees transferring to sensitive positions.*
Security awareness and safety training for employees needs strengthening	*Several employees were identified who had not completed the required prior year security awareness refresher-training course. Also, data center staff had not received periodic safety training in emergency, fire, water and alarm incident procedures since 2 years prior.*	*Management should ensure that all employees complete their annual training requirements. Further, officials should ensure that training in emergency, fire, water, and alarm incident procedures is conducted annually for new and existing data center employees.*
New hires did not receive new employee orientation	*A significant number of a sample of new hires did not receive New Employee Orientation, which consists of policy training, data training on the Data Classification and Handling System, and training on the acceptable use of the internet and communication systems.*	*Management should fully implement mandatory new hire training for all employees to ensure that employees are aware of their security responsibilities. Additionally, we recommend more stringent monitoring of new hire training for all employees, including penalties for those employees who do not attend. Monitoring should include periodic sampling of compliance by management.*
Annual security awareness training refresher course is not mandatory	*Our review of the annual security awareness training refresher course noted that there has not been*	*We recommend that management establish a mandatory requirement for 100% participation of the annual security awareness refresher training course for all associates and contractors*

Finding	*Issue*	*Suggested Remediation*
	*an establishment of a **mandatory** requirement for all employees/contractors to participate in the refresher course.*	*relative to their job functions and their access to sensitive information. Additionally, we recommend monitoring and tracking compliance of this requirement for all associates and contractors. Like the audit team, management should periodically select a sample of employees during the year to check ongoing compliance.*
The incident response capability needs strengthening	*During our review of the Computer Incident Response Capability we noted that an understanding of the constituency being served is unavailable, as well as evidence of the Incidence Response Team qualifications and training.*	*We recommend that management review their incident response capability and ensure that an Incidence Response Team is established with the necessary qualifications, skills, knowledge and abilities to respond to security incidents. Additionally, the Incidence Response Team should be trained, at a minimum, annually on emergency/incidence response and procedures. That training should be monitored and tracked for 100% participation of all IRT members.*
Job rotation and vacation policy does not exist	*A formal policy mandating periodic job rotations and vacation for personnel does not exist.*	*We recommend that management incorporate a formal job rotation and vacation policy so that responsibilities can be re-assigned to different individuals. Should neither of the above two measures exist, we recommend the monitoring of employee activities who are exposed to sensitive data over extended periods in order to reduce potential security risks.*
Weaknesses identified in termination process	*During our review of Exit Interview checklists for a sample of terminations, we noted that checklists were not completed for a large percentage of terminations.*	*We recommend that the enforcement of the termination policy/procedures be strengthened. Management should be held accountable for completion of termination checklist.*

3.6 Periodic Review and Testing of Controls

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

3.7 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

*The **development and implementation of an entity-wide security plan** is the foundation for building a secure information processing environment. The objective of **development and implementation of an entity-wide security plan** is to provide a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an entity's computer related controls.*

*Through **the development and implementation of an effective entity-wide security plan**, security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud.*

The implementation of effective IT controls should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table E-6. Applicable FISCAM Controls

FISCAM General Controls
SP-1 Periodically Assess Risks
SP-2 Document an entity-wide security program plan
SP-2.1 A security plan is documented and approved
SP-2.2 The plan is kept current
SP-3 Establish a security management structure and clearly assign security responsibilities
SP-3.1 A security management structure has been established
SP-3.2 Information security responsibilities are clearly assigned
SP-3.3 Owners and users are aware of security policies
SP-3.4 An incident response capability has been implemented
SP-4 Implement effective security related personnel policies
SP-4.1 Hiring, transfer, termination, and performance policies address security
SP-4.2 Employees have adequate training and expertise
SP-5 Monitor the security program's effectiveness and make changes as needed
SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them
SP-5.2 Management ensures that corrective actions are effectively implemented
AC-1 Classify information resources according to their criticality and sensitivity
AC-1.1 Resource classifications and related criteria have been established
AC-1.2 Owners have classified resources
SD-1 Segregate incompatible duties and establish related policies
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties
SD-1.2 Job descriptions have been documented
SD-1.3 Employees understand their duties and responsibilities

Table E-7. Applicable NIST SP 800-53 Controls

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
	Family: Access Control	
	AC-1	*Access Control Policy and Procedures*
	Family: Awareness and Training	
	AT-1	*Security Awareness and Training Policy and Procedures*
	AT-2	*Security Awareness*
	AT-3	*Security Training*
	AT-4	*Security Training and Records*
	Family: Audit and Accountability	
	AU-1	*Audit and Accountability Policy and Procedures*
	Family: Certification, Accreditation, and Security Assessments	

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
	CA-1	*Certification, Accreditation, and Security Assessment Policies and Procedures*
SP-5.1	*CA-2*	*Security Assessments*
CC-2.1	*CA-3*	*Information System Connections*
CC-2.1	*CA-4*	*Security Certification*
SP-5.1, SP-5.2	*CA-5*	*Plan of Action and Milestones*
	CA-6	*Security Accreditation*
	CA-7	*Continuous Monitoring*
	Family: Configuration Management	
	CM-1	*Configuration Management Policy and Procedures*
	Family: Contingency Planning	
	CP-1	*Contingency Planning Policy and Procedures*
	Family: Identification and Authentication	
	IA-1	*Identification and Authentication Policy and Procedures*
	Family: Incident Response	
	IR-1	*Incident Response Policy and Procedures*
	Family: Maintenance	
	MA-1	*System Maintenance Policy and Procedures*
	Family: Media Protection	
	MP-1	*Media Protection Policy and Procedures*
	Family: Physical and Environmental Protection Policy and Procedures	
	PE-1	*Physical and Environmental Protection Policy and Procedures*
	Family: Planning	
	PL-1	*Security Planning Policy and Procedures*
SP-2.1	*PL-2*	*System Security Plan*
SP-2.1	*PL-3*	*System Security Plan Update*
	PL-4	*Rules of Behavior*
	PL-5	*Privacy Impact Assessment*
	Family: Personnel Security	
	PS-1	*Personnel Security Policy and Procedures*
SD-1.2	*PS-2*	*Position Categorization*
SP-4.1	*PS-3*	*Personnel Screening*
SP-4.1	*PS-4*	*Personnel Termination*
SP-4.1	*PS-5*	*Personnel Transfer*
SP-4.1	*PS-6*	*Access Agreements*
SP-4.1	*PS-7*	*Third-Party Personnel Security*
	PS-8	*Personnel Sanctions*
	Family: Risk Assessment	
	RA-1	*Risk Assessment Policy and Procedures*
SP-1, AC-1.1,	*RA-2*	*Security Categorization*

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
AC-1.2		
SP-1	*RA-3*	*Risk Assessment*
SP-1	*RA-4*	*Risk Assessment Update*
	RA-5	*Vulnerability Scanning*
	Family: System and Services Acquisition	
	SA-1	*System and Services Acquisition Policy and Procedures*
	Family: System and Communication Protection	
	SC-1	*System and Communications Protection Policies and Procedures*
	Family: System and Information Integrity	
	SI-1	*System and Information Integrity Policies and Procedures*

4.0 CMS Guidelines on Application Programmers' Access to Application Data and Source Code

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

4.1 Overview

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is controls around ***access for application programmers to application data and source code.***

This guideline will:

- *Provide a high level understanding of controls around* ***access for application programmers to application data and source code,***
- *Facilitate the identification of IT controls, in key Federal guidelines and standards, which directly concern* ***access for application programmers to application data and source code,*** *and*
- *Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.*

4.2 Introduction to Access Controls for Application Programmers to Application Data and Source Code

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Business Partners Systems Security Manual (BPSSM) defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

General Accounting Office' (GAO) Federal Information Systems Controls Audit Manual (FISCAM) states that "Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."

A key component of comprehensive access controls for application programmers is 'Segregation of Duties'. FISCAM defines 'Segregation of duties' as controls that describe how work responsibilities should be segregated so that one person does not have access to or control over all of the critical stages of an information handling process. For instance; while a representative of the user community may initiate requests to changes in system capabilities, computer

programmers should not be able to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more organizational groups to ensure independence and objective checks and balances. These controls can be enforced through automated and/or manual measures.

4.3 Risks of Non-compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

FISCAM states that "Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or 'turned off' or that processing irregularities or malicious code could be introduced." Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- *A knowledgeable programmer could surreptitiously modify program code to provide a means of bypassing controls to gain access to sensitive data;*

- *The wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or*

- *A virus could be introduced, inadvertently or on purpose, that disrupts processing.*

FISCAM states that "inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed." FISCAM provides the following example of potential consequences of inadequate controls around segregation of duties:

> *A computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.*

Within appendix C of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. 'Separation of Duties' is listed as a key safeguard against employee fraud. For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix C of the BPSSM.

4.4 Specific Controls to be Implemented

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All controls documented in the BPSSM are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls

may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, ***unless other compensatory controls are in place, which satisfy the control objective.***

Tables E-9 and E-10 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to ***application programmers' access to application data and source code****. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-9. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-10.*

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-10 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to ***application programmers' access to application data and source cod****e. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.*

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-10 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-10, the corresponding FISCAM control in Table E-9, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines ***around application programmers' access to application data and source code.***

4.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Table E-8 provides a listing of sample instances of non-compliance with controls around ***application programmers' access to application data and source code,*** *based on prior controls reviews and audits. Specifically, the table lists the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue take into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.*

Table E-8. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	*Issue*	*Suggested Remediation*
Access to database security tables	*Programmers and contractors have update access to the database security tables of selected systems.*	*Update access to the application database security tables should be removed for programmers and contractors. The access rights limitation documentation must be available to all key security positions including, but not limited to, security administrators, system administrators, and various security compliance monitoring positions.*
Change control process	*While reviewing the Software Quality Assurance (SQA) document, and completing our detailed change control testing, we noted that the procedures for implementing SQA Policy do not contain specific retention and disposal guidelines for the electronic or paper Change Control artifacts (i.e. Project Initiation form, Test Certification Statement, Problem Report, Testing [plan and results], Validation Readiness Review, Implementation Readiness Review, and ENDEVOR Data related to the change).*	*SQA should be improved to ensure that it provides specific retention and disposal guidelines for all artifacts including the Project Initiation form, Test Certification Statement, Problem Report, Testing (plans and results), Validation*

Finding	Issue	Suggested Remediation
		Readiness Review, Implementation Readiness Review, and ENDEVOR Data related to the change.
Compliance with change control procedures	During the completion of our detailed testing related to the Change Control procedures in use, we noted the following issues: Of the changes reviewed for different systems, the standard Change Control procedures were not consistently followed. Specifically, the following was noted: The application personnel for one system did not use the Project Initiation/Project Release Notice and the Release Notification Package. The standard change initiation form was not used for the changes we reviewed for one of the systems. The Initiation form and the Release Notification Package were not provided to the Software Quality Assurance Point of Contact (SQA POC) for any of the changes reviewed. Evidence of testing was not available for the changes selected for some of the systems.	All changes to applications should consistently follow the official change control policies and procedures outlined in the SQA document. Management should periodically select a sample of changes for high impact systems to check that procedures are being observed. The entity performing the validation should be organizationally independent of the application being reviewed.
Developer movement of changes into production	During our review of the ENDEVOR change control software configuration, we noted the following issues: Application programmers for one application system can cause, through the ENDEVOR approval process, software changes to be placed in the production environment without the knowledge or approval of the application Business Owners. The current ENDEVOR configuration, as it relates to this application system, does not require Business Owner approval for movement of changes into the production environment. The application programmers for another application system are also the application Business Owners. This results in a lack of separation of duties between the personnel making changes to the application, and the personnel approving those changes for movement into the production environment.	Application programmers for the application system, should be required to attain Business Owner approval for movement of changes into the production environment. For the one system discussed under issues, a group other than the programmers should be required to approve all application changes before they are moved into the production environment.

Finding	*Issue*	*Suggested Remediation*
Production systems logical access	*The operations attribute, which allows special privileges under the security software on the mainframe, including the ability to bypass security and/or change access for some other users, was assigned to a person who no longer needs the attribute to perform job responsibilities. This person was a mainframe systems programmer, but now supports mid-range systems.* *ALTER access to production data has been granted to numerous users, including systems analysts and application programmers. ALTER access by systems analysts and application programmers represents a segregation of duties issue for these users who could use this access to change data outside of the application processes.* *Access to bypass tape dataset security checking had been assigned to a number of users, including numerous systems analysts and application programmers. Such access violates the concept of segregation of duties and allows all of these users to access and update any tape dataset.*	*Management should ensure that:* *User access assigned is periodically reviewed and adjusted as necessary, including review of access to systems software files.* *Access is only assigned on the basis of least privilege to perform job responsibilities.* *Access assigned ensures segregation of duties is enforced.* *Access assignment processes are consistently performed through the use of formal written standard procedures that define the processes to assign, review or modify the access of <u>all</u> system users.* *Ongoing review and monitoring of user activities is performed for the use of sensitive utility programs or access to system datasets.*
Production systems logical access	*Some of the individuals authorized to move application changes into production were application programmers.*	*Application programmer access to the production environment should be removed. Furthermore, access provided to the programmers should be limited to their job*

Finding	Issue	Suggested Remediation
		responsibility.
Applications programmers access to production code and data	*During our audit we noted the following deficiencies:* *Programmers have access to network-based applications including production code and production data.* *Programmer access to both older and new network-based application production code and data includes read, write, and delete access rights.*	*Create and maintain a change management process that controls all network-based application environments.* *Create separate test/development environment for network-based applications.* *Build application access controls into network-based applications.* *Alter programmer access rights to production code and data for network-based applications.*

4.6 Periodic Review and Testing of Controls

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security

control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

4.7 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

*Controls around **application programmers' access to application data and source code** help to ensure that only authorized programs and authorized modifications are implemented. Segregation of duties, a key component of these controls, facilitate the separation of work responsibilities such that one person does not have access to or control over all of the critical stages of an information handling process such that unauthorized data access and modification is not prevented or detected.*

*Through the implementation of effective controls around **application programmers' access to application data and source code** security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud.*

The implementation of these controls should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table E-9. Applicable FISCAM Controls

FISCAM General Controls
SP-1 Periodically Assess Risks
AC-1 Classify information resources according to their criticality and sensitivity
AC-1.1 Resource classifications and related criteria have been established

AC-1.2 Owners have classified resources
AC-2 Maintain a current list of authorized users and their access authorized
AC-2.1 Resource owners have identified authorized users and their access authorized
AC-2.2 Emergency and temporary access authorization is controlled
AC-2.3 Owners determine disposition and sharing of data
AC-3.2 Adequate logical access controls have been implemented
A. Passwords, tokens, or other devices are used to identify and authenticate users
B. Identification of access paths
C. Logical controls over data files and software programs
D. Logical controls over a database
E. Logical controls over telecommunications access
CC-1 Processing features and program modifications are properly authorized
CC-1.1 A system development life cycle methodology(SDLC) has been implemented
CC-1.2 Authorizations for software modifications are documented and maintained
CC-1.3 Use of public domain and personal software is restricted
CC-2 Test and approve all new and revised software
CC-2.1 Changes are controlled as programs progress through testing to final approval
CC-2.2 Emergency changes are promptly tested and approved
CC-2.3 Distribution and implementation of new or revised software is controlled
CC-3 Control software libraries
CC-3.1 Programs are labeled and inventoried
CC-3.2 Access to program libraries is restricted
CC-3.3 Movement of programs and data among libraries is controlled
SS-1 Limit access to system software
SS-1.1 Access authorizations are appropriately limited
SS-2 Monitor access to and use of system software
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities
SS-3 Control system software changes
SS-3.1 System software changes are authorized, tested and approved before implementation
SS-3.2 Installation of system software is documented and reviewed
SD-1 Segregate incompatible duties and establish related policies
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties
SD-1.2 Job descriptions have been documented
SD-1.3 Employees understand their duties and responsibilities
SD-2 Establish access controls to enforce segregation of duties
SD-2.1 Physical and logical access controls have been established
SD-2.2 Management reviews effectiveness of control techniques
SD-3 Control personnel activities through formal operating procedures and supervision and review
SD-3.1 Formal procedures guide personnel in performing their duties
SD-3.2 Active supervision and review are provided for all personnel

Table E-10. Applicable NIST SP 800-53 Controls

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
	Family: Access Control	
	AC-1	*Access Control Policy and Procedures*
AC-2, AC-3.2	*AC-3*	*Access Enforcement*
AC-3.2, SD-1.2	*AC-5*	*Separation of Duties*
	Family: Awareness and Training	
	AT-1	*Security Awareness and Training Policy and Procedures*
	AT-2	*Security Awareness*
	AT-3	*Security Training*
	AT-4	*Security Training and Records*
	Family: Configuration Management	
	CM-1	*Configuration Management Policy and Procedures*
CC-2.3, CC-3.1, SS-1.2	*CM-2*	*Baseline Configuration*
SS-3.2, CC-2.2	*CM-3*	*Configuration Change Control*
SS-3.1, SS-3.2, CC-2.1	*CM-4*	*Monitoring Configuration Changes*
SD-1.1, SS-1.2, SS-2.1	*CM-5*	*Access Restrictions for Change*
	CM-6	*Configuration Settings*
	CM-7	*Least Functionality*
	Family: Risk Assessment	
	RA-1	*Risk Assessment Policy and Procedures*
SP-1, AC-1.1, AC-1.2	*RA-2*	*Security Categorization*
SP-1	*RA-3*	*Risk Assessment*
SP-1	*RA-4*	*Risk Assessment Update*

5.0 CMS Guidelines on Change Management Procedures

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

5.1 Overview

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A key component of effective information technology (IT) controls is security, and a key foundation of comprehensive security controls is ***change management procedures.*** *Included in the controls around change management are requirements for maintaining change management documentation.*

This guideline will:

- *Provide a high level understanding of **change management procedures**,*
- *Facilitate the identification of IT controls, in key Federal guidelines and standards, which are directly related **change management procedures,** and*
- *Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.*

5.2 Introduction to Change Management Procedures

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Business Partners Systems Security Manual (BPSSM) defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

General Accounting Office' (GAO) Federal Information Systems Controls Audit Manual (FISCAM) states that:

> *"Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."*
>
> *"Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing systems changes. However, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change."*
>
> *"The use of standardized change request forms helps ensure that requests are clearly communicated and that all approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected."*

5.3 Risks of Non-compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

In discussing change controls, FISCAM states that "Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or 'turned off' or that processing irregularities or malicious code could be introduced." Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- *A knowledgeable programmer could surreptitiously modify program code to provide a means of bypassing controls to gain access to sensitive data;*

- *The wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or*

- *A virus could be introduced, inadvertently or on purpose, that disrupts processing.*

Within appendix C of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. Manual controls, such as required maintenance of hardcopy forms/documentation (e.g., change control approvals), are discussed as a key safeguard against employee fraud. For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix C of the BPSSM.

5.4 Specific Controls to be Implemented

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

All controls documented in the BPSSM are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, ***unless other compensatory controls are in place, which satisfy the control objective.***

Tables E-12 and E-13 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to change management procedures. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-12. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-13.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-13 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to ***change management procedures.*** *Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of*

cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-13 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-13, the corresponding FISCAM control in Table E-12, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines around ***change management procedures.***

Table E-11. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	***Issue***	***Suggested Remediation***
Evidence of program staff attendance of SDLC training.	*Management could not produce the sign-in sheets for the SDLC class held in the prior year.*	*Document and maintain evidence that the programming staff attended the SDLC class. The SDLC class should include (but not be limited to) the following change management: related topics:* *Documented authorizations for software modifications* *Controls around program changes as they progress through testing to final approval* *Testing and approval of emergency changes* *Controls around distribution and implementation of new or revised software* *Program labeling*

Finding	*Issue*	*Suggested Remediation*
Change control process requires clarifications	*While reviewing the Software Quality Assurance (SQA) document, and completing our detailed change control testing, we noted that procedures for implementing SQA policy do not contain specific retention and disposal guidelines for the electronic or paper Change Control artifacts (i.e. Project Initiation form, Test Certification Statement, Problem Report, Testing [plan and results], Validation Readiness Review, Implementation Readiness Review, and ENDEVOR Data related to the change).*	*SQA should be improved to ensure that it provides specific retention and disposal guidelines for all controls documentation including the Project Initiation form, Test Certification Statement, Problem Report, Testing (plans and results), Validation Readiness Review, Implementation Readiness Review, and ENDEVOR Data related to the change*
Compliance with change control procedures	*During the completion of our detailed testing related to the Change Control procedures in use, we noted the following issues:* *Of the changes we reviewed for different systems, the standard Change Control procedures were not consistently followed. Specifically, the following was noted:* *The application personnel for one system did not use the Project Initiation/Project Release Notice and the Release Notification Package.* *The standard change initiation form was not used for the changes we reviewed for one of the systems.* *The Initiation form and the Release Notification Package were not provided to the Software Quality Assurance Point of Contact (SQA POC) for any of the changes reviewed.* *Evidence of testing was not available for the changes selected for some of the systems.*	*All changes to applications should consistently follow the official change control policies and procedures outlined in the SQA document.* *Management should periodically select a sample of changes for high impact systems to check that procedures are being observed. The entity performing the validation should be organizationally independent of the application being reviewed.*
Developer movement of changes into production	*During our review of the ENDEVOR change control software configuration, we noted the following issues:* *Application programmers for one application system can cause, through*	*Application programmers for the application system should be required to attain Business Owner approval for movement of changes into the production environment.*

Finding	Issue	Suggested Remediation
	the ENDEVOR approval process, software changes to be placed in the production environment without the knowledge or approval of the application Business Owners. The current ENDEVOR configuration, as it relates to this application system, does not require Business Owner approval for movement of changes into the production environment. The application programmers for another application system are also the application Business Owners. This results in a lack of separation of duties between the personnel making changes to the application, and the personnel approving those changes for movement into the production environment.	For the system discussed under issues, a group other than the programmers should be required to approve all application changes before they are moved into the production environment.
Application change control procedures	Our testing disclosed the following issues: Some change control records reviewed had the same individual approve both approval forms at the same time, contradictory to the procedure in place. The change controls procedures discuss the unit and user testing. However, these procedures do not require the testers, both the unit and/or user, to maintain and approve this testing before it receives the final approval and is entered into production.	Require change requests to be authorized by unique and appropriate individuals. A standard for performing unit and user testing, maintaining the results, and approving the completion of this testing should be included within the change control procedures. This standard should be communicated and followed by the appropriate personnel.
Mainframe systems software controls	The "LNKAUTH=LNKLST" setting (instead of "LNKAUTH=APFTAB") was inappropriately in effect as defined within the IEASYS00 member of 'SYS1.PARMLIB'. In addition to all libraries defined in the Authorized Program Facility (APF) List, this setting inappropriately grants APF-authorization to all libraries defined in the Link List. APF authorized libraries contain programs that are allowed to bypass the	With the next operating system upgrade (i.e., rollout of the next operating system shell), change the LNKAUTH parameter to "LNKAUTH=APFTAB", making the PROGxx members of 'SYS1.PARMLIB' the single-source of APF-authorized datasets (explicitly defined in the APF List) and using the LNKLSTxx member of 'SYS1.PARMLIB' (or

Finding	Issue	Suggested Remediation
	security software (RACF) on the mainframe. Programs executed from such libraries could gain update access to all programs and data on the system and should therefore be limited to only those programs requiring this ability to execute and perform their intended function. *Through analysis of the Link List and the APF List libraries, we noted the following:* *Many libraries were defined to both the Link List and to the APF List.* *Some libraries were defined to the Link List, but not to the APF List, thereby attaining APF-authorization via the LNKAUTH=LNKLST setting.* *Numerous libraries were defined to the APF List, but not the Link List.*	*DYNAMIC LNKLST) only for its primary purpose of being the default search path for executed programs and not as a secondary APF List.*
Application change management	*Change management procedures were outdated. Policies for local code procedures including emergency changes, written and published by the contractor, do not reflect the current implementation processes for emergency changes.* *All of the changes sampled did not have documented authorization forms.*	*Emergency change procedures, documented in the local code procedures, should be updated to reflect the current process for implementation of emergency changes.* *Management should ensure that request forms are completed and authorized before promoting a change into production. The request forms should be maintained for audit trail purposes.*

5.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

*Table E-12 provides a listing of sample instances of non-compliance with **change management** controls based on prior controls reviews and audits. Specifically, the table lists the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected*

instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue take into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.

5.6 Periodic Review and Testing of Controls

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

5.7 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Change management procedures are controls that help to ensure that only authorized programs and authorized modifications are implemented. Documentation of these processes is critical in that it allow CMS management to identify who requested a change to the system, why the change was requested (business/operational justification), what the exact change was, who made the change, and who approved the change. Through the implementation of effective change

management procedures, security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud.

The implementation of these controls should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table E-12. Applicable FISCAM Controls

FISCAM General Controls
SP-1 Periodically Assess Risks
CC-1 Processing features and program modifications are properly authorized
CC-1.1 A system development life cycle methodology(SDLC) has been implemented
CC-1.2 Authorizations for software modifications are documented and maintained
CC-1.3 Use of public domain and personal software is restricted
CC-2 Test and approve all new and revised software
CC-2.1 Changes are controlled as programs progress through testing to final approval
CC-2.2 Emergency changes are promptly tested and approved
CC-2.3 Distribution and implementation of new or revised software is controlled
CC-3 Control software libraries
CC-3.1 Programs are labeled and inventoried
CC-3.2 Access to program libraries is restricted
CC-3.3 Movement of programs and data among libraries is controlled
SS-3 Control system software changes
SS-3.1 System software changes are authorized, tested and approved before implementation
SS-3.2 Installation of system software is documented and reviewed

Table E-13. Applicable NIST SP 800-53 Controls

Corresponding FISCAM Control	***NIST 800-53 Recommended Security Controls***	
	Family: Configuration Management	
	CM-1	*Configuration Management Policy and*

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
		Procedures
CC-2.3, CC-3.1, SS-1.2	*CM-2*	*Baseline Configuration*
SS-3.2, CC-2.2	*CM-3*	*Configuration Change Control*
SS-3.1, SS-3.2, CC-2.1	*CM-4*	*Monitoring Configuration Changes*
SD-1.1, SS-1.2, SS-2.1	*CM-5*	*Access Restrictions for Change*
	CM-6	*Configuration Settings*
	CM-7	*Least Functionality*

6.0 CMS Guidelines on Implementation and Maintenance of Security Configuration Templates

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

6.1 Overview

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is the ***implementation and maintenance of security configuration templates.***

This guideline will:

- *Provide a high level understanding of* ***implementation and maintenance of security configuration templates,***
- *Facilitate the identification of IT controls, in key Federal guidelines and standards, which are directly related to the* ***implementation and maintenance of security configuration templates,*** *and*
- *Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.*

6.2 Introduction to the Implementation and Maintenance of Security Configuration Templates

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Business Partners Systems Security Manual (BPSSM) and the General Accounting Office' (GAO) Federal Information Systems Controls Audit Manual (FISCAM) define configuration management as "the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system."

The BPSSM also states "The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires National Institute of Standards and Technology (NIST) to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government. The guidelines and checklists are developed to help system operators configure security within these systems to the highest level possible."

NIST has produced Special Publication 800-70 "Security Configuration Checklists Program for IT Products - Guidance for Checklist Users and Developers" to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.

NIST also states that "a security configuration checklist" (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular operational environment. It could also include templates or automated scripts and other procedures. Checklists can be created by IT vendors for their own products or created by other organizations such as consortia, academia, open source, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products."

6.3 Risks of Non-compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

In discussing security configuration templates and checklists, NIST states that

> *"Vulnerabilities in IT products are discovered on an almost daily basis, and many ready-to-use exploits are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default, so many IT products are immediately vulnerable out-of-the-box."*

Some of the risks inherent in not implementing and maintaining common security templates, according to NIST, include:

- *the inconsistent application of security configurations across all vulnerable platforms could cause a single system to be compromised and serve as an entry point to the larger network,*

- *lack of common security configuration standards would increase the time required to research and apply security settings to systems individually.*

The potential consequences of inconsistent or lack of use of security configuration templates or checklists are identical to those associated with inadequate access controls, which are indicated in FISCAM.

6.4 Specific Controls to be Implemented

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Security configuration templates take one of two forms. Some configuration templates are software-based in the form of a file or files which contain predetermined security settings which can be applied to single or multiple systems in an automated fashion. The other type of configuration template is policy-based and in the form of a checklist or recommendations guide, applied manually to the system during initial build and deployment.

Both NIST and the NSA provide security configuration checklists and security configuration guides for multiple operating systems and applications. Additionally, Security Technical Implementation Guides (STIGs) are published as tools to assist in the improvement of the security of Department of Defense (DOD) information systems. They are created using the principle that the most effective way to improve security in information systems is to include security in the initial design and development. As such, they provide the technical security policies, requirements, and implementation details for applying security concepts to information systems.

According to the BPSSM, CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program. Specifically, MACs and EDCs are required to start with these baseline configurations listed in the Security Technical Implementation Guides (STIGs) and should document any exceptions based on environment-specific implementation. The use of STIGs will:

- *Reduce the likelihood of successful intrusions or attacks;*
- *Facilitate secure configuration of systems prior to network deployment;*
- *Assist with monitoring systems for on-going conformance with security configurations*

Section 3.10.1 of this document (BPSSM) contains a list of applicable STIGs and their location.

Some operating system vendors include robust configuration management capabilities within the software. For example, Microsoft has included multiple methods to natively manage the configuration of Windows systems. The Windows Security Configuration Manager tool set allows administrators to create, apply and edit the security for local computers, organizational units, or domains. Windows also allows the construction and application of software-based security configuration templates. Microsoft states,

"With the Security Templates snap-in for Microsoft Management Console, administrators can create a security policy for computers or for networks. It is a single point of entry where the full range of system security can be taken into account. The Security Templates snap-in does not introduce new security parameters; it simply organizes all existing security attributes into one place to ease security administration."

The BPSSM states that "Business partners are ***required*** *to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology." The relevant FISCAM and*

NIST SP 800-53 controls identified to mitigate the risks discovered in the risk assessment can then be used to develop effective security configuration templates. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All controls documented in the BPSSM are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, ***unless other compensatory controls are in place, which satisfy the control objective.***

Tables E-15 and E-16 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to the ***implementation and maintenance of security configuration templates****. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-15. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-16.*

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-16 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to the ***implementation and maintenance of security configuration templates****. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.*

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-16 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-16, the corresponding FISCAM control in Table E-15, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines related to the ***implementation and maintenance of security configuration templates****.*

6.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Table E-14 provides a listing of sample instances of non-compliance with the ***implementation and maintenance of security configuration templates*** *based on prior controls reviews and audits. Specifically, the table lists the findings and recommended course of action for selected cases of non-compliance. In these cases non-compliance refers not only to controls which were not in place, but also to controls which would have been applied if security configuration templates had been used to configure those systems. The findings in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue take into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.*

Table E-14. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	*Issue*	*Suggested Remediation*
Default or blank passwords exist for user accounts.	*Malicious users could gain the ability to gain access to systems.*	*Unique passwords should be created for each account.*
The rlogin service is enabled.	*The r-services, in conjunction with the /etc/hosts.equiv file and individual .rhosts files, place a system at risk. They allow users to log in or execute commands from a trusted system without re-authenticating.*	*The Berkley r-services (e.g., rexec, rlogin, rsh) should be disabled unless there is a strong business need. One potential alternative is to use SSH for remote access.*
The Simple Mail Transport Protocol (SMTP) service appears to allow relaying.	*Mail servers should not allow relaying as this could allow the server to be used to falsify e-mails or send SPAM, potentially opening the organization up to liability.*	*Disable SMTP if not needed or configure to disallow relaying for any users not coming from organization owned networks.*
There are users whose passwords never expire. In addition, some users cannot change their passwords.	*This setting is not recommended unless this is a service account, as it leads to less frequent password changes*	*Enable the setting to make these users change their passwords on a regular basis.* *Remove the Password Never Expires option*
The minimum password length, maximum password age, password history length, and minimum password age are not set accordance with policy	*Insufficient password policies can allow attackers to compromise accounts with weak passwords.*	*If a password policy does not currently exist, a strong, enterprise wide password policy should be developed. This password policy should be enforced on all servers and applications in the environment.*
Multiple default Microsoft Internet Information Services (IIS) files that result in exposing system information are present on the system.	*These files may provide sensitive information about medical clients, usernames, and passwords or allow files to be written to the system.*	*Less secure default settings should be changed for all applicable systems. All unnecessary services and applications should be removed.*
Unsecured network services, such as Telnet and FTP are enabled.	*Passwords are transmitted across the network in clear text when a user is logging into these services and could be obtained by a malicious user.*	*Unnecessary services should be removed or disabled when not in use.* *Encryption of logins and passwords should be enabled*

Finding	Issue	Suggested Remediation
		wherever possible.
Web pages containing system information do not require authentication.	Browsing of sensitive web pages which do not require authentication may provide sensitive information to compromise the host.	Access to sensitive information should be restricted to authorized users only.
Null sessions were established with numerous Windows systems.	If not appropriately restricted, null sessions may allow an unauthorized user to obtain sensitive information, including user names and system information.	Null sessions should have restrictions placed on their use, including but not limited to restricted access, session timeouts, and access logging.
A default version of Microsoft SQL Server 2000 is installed.	Microsoft SQL Server 2000 is vulnerable to a heap buffer overflow in the SQL Server Resolution Service, which is used to direct client requests to the proper port when multiple instances of the SQL Server are running on the same system. By sending a specially-crafted request to UDP port 1434 consisting of a byte set to 0x08 followed by an overly long string and a colon character (:), a remote attacker could overflow a buffer and cause the SQL Server service to crash or execute arbitrary code on the system with the same privileges as the SQL Server.	All affected servers should be patched for this vulnerability, as listed in Microsoft Security Bulletin MS02-039.
Users or shares were detected using a null session.	A null session is a NetBIOS connection established with a zero length string as user, password, and domain name, which is designed to enable enumeration of shares and users. This capability has always been present in Windows NT, but was discovered to allow access to the registry with the same level of permissions as the Everyone group. It is a medium risk vulnerability (similar to finger) that allows users and shares to be enumerated. An attacker could use this information to learn more about the network architecture to support a future attack.	Apply the latest Windows NT 4.0 Service Pack (SP3 or later), available from the Windows NT Service Packs Web page. Users should also remove all unnecessary shares, and restrict anonymous connections.

6.6 Periodic Review and Testing of Controls

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems (which all CMS systems are considered to be). Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

FISCAM refers to the maintenance of security configuration templates more specifically when it discusses maintaining System Security Plans. It states,

> *"To be effective, the policies and plan should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks and, therefore, may be ineffective."*

The BPSSM states that "CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity." As requirements change or arise from the configuration management program, these new changes should be reflected by changes in the appropriate template.

6.7 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

According to NIST, while the use of security configuration checklists and templates can greatly improve overall levels of security in organizations, no checklist can permit a system or a product to become 100 % secure. However, use of checklists and templates that emphasize hardening of systems against flaws or bugs inherent in software will typically result in greater levels of product security and protection from future threats.

The threats facing networks today are dynamic and persistent. New systems not only need to be secure before becoming operational, but the standards used to configure them also need to be continually updated to keep pace with new and changing threats.

The implementation of these controls should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table E-15. Applicable FISCAM Controls

FISCAM General Controls
SP-1 Periodically Assess Risks
SP-2 Document an entity-wide security program plan
SP-2.1 A security plan is documented and approved
SP-2.2 The plan is kept current
SP-5 Monitor the security program's effectiveness and make changes as needed
SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them
CC-1 Processing features and program modifications are properly authorized
CC-1.2 Authorizations for software modifications are documented and maintained
CC-2 Test and approve all new and revised software
CC-2.1 Changes are controlled as programs progress through testing to final approval
SS-2 Monitor access to and use of system software
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities
SS-3 Control system software changes
SS-3.1 System software changes are authorized, tested and approved before implementation
SS-3.2 Installation of system software is documented and reviewed

Table E-16. Applicable NIST SP 800-53 Controls

Corresponding FISCAM Control	NIST 800-53 Recommended Security Controls	
	Family: Access Control	
	AC-1	Access Control Policy and Procedures
	Family: Certification, Accreditation, and Security Assessments	
SP-5.1	CA-2	Security Assessments
SP-5.1, SP-5.2	CA-5	Plan of Action and Milestones
	CA-7	Continuous Monitoring
	Family: Configuration Management	
	CM-1	Configuration Management Policy and Procedures
CC-2.3, CC-3.1, SS-1.2	CM-2	Baseline Configuration
SS-3.2, CC-2.2	CM-3	Configuration Change Control
SS-3.1, SS-3.2, CC-2.1	CM-4	Monitoring Configuration Changes
SD-1.1, SS-1.2, SS-2.1	CM-5	Access Restrictions for Change
	CM-6	Configuration Settings
	CM-7	Least Functionality
	Family: Contingency Planning	
	CP-1	Contingency Planning Policy and Procedures

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
SC-2.1	*CP-10*	*Information System Recovery and Reconstitution*
	Family: Identification and Authentication	
	IA-1	*Identification and Authentication Policy and Procedures*
	Family: Maintenance	
	MA-1	*System Maintenance Policy and Procedures*
	Family: Planning	
	PL-1	*Security Planning Policy and Procedures*
SP-2.1	*PL-2*	*System Security Plan*
SP-2.1	*PL-3*	*System Security Plan Update*
	Family: Risk Assessment	
	RA-1	*Risk Assessment Policy and Procedures*
SP-1, AC-1.1, AC-1.2	*RA-2*	*Security Categorization*
SP-1	*RA-3*	*Risk Assessment*
SP-1	*RA-4*	*Risk Assessment Update*
	RA-5	*Vulnerability Scanning*
	Family: System and Services Acquisition	
CC-2.1	*SA-5*	*Information System Documentation*
SS-3.2, SP-2.1	*SA-6*	*Software Usage Restrictions*
	SA-8	*Security Design Principles*
	SA-9	*Outsourced Information System Services*
CM-3	*SA-10*	*Developer Configuration Management*
CM-3	*SA-11*	*Developer Security Testing*
	Family: System and Communication Protection	
	SC-1	*System and Communications Protection Policies and Procedures*
	Family: System and Information Integrity	
	SI-1	*System and Information Integrity Policies and Procedures*

7.0 CMS Guidelines on Testing Process for the SANS Top 20 Internet Security Vulnerabilities

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

7.1 Overview

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls includes a ***Testing Process for the SANS Top 20 Internet Security Vulnerabilities****. This guideline will:*

- *Provide a high level understanding of the SANS Top 20 Internet Security Vulnerabilities,*
- *Facilitate the identification of IT controls, in key Federal guidelines and standards, which are directly related to Testing for the SANS Top 20 Internet Security Vulnerabilities, and*
- *Provide a sample of prior instances of lack of identification and remediation of the SANS Top 20 Internet Security Vulnerabilities and recommended testing approaches.*

7.2 Introduction to Testing for the SANS Top 20 Internet Security Vulnerabilities

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

General Accounting Office' (GAO) Federal Information Systems Controls Audit Manual (FISCAM) states that an important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. To implement an effective security plan, top management should monitor its implementation and adjust the plan in accordance with changing risk factors. Over time, policies and procedures may become inadequate because of changes in operations or deterioration in the degree of compliance. Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.

OMB Circular A-130, Appendix III, requires that Federal agencies review the security of their general support systems and major applications at least once every 3 years or sooner, if significant modifications have occurred or where the risk and magnitude of harm are high.

In addition, the Federal Managers Financial Integrity Act (FMFIA) of 1982 and OMB Circular A-123 require agencies to annually assess their internal controls, including computer-related controls, and report any identified material weaknesses to the President and the Congress.

When significant weaknesses are identified, the related risks should be reassessed, appropriate corrective actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. This is an important aspect of management's risk management responsibilities. In addition to modifying written policies to correct identified problems, implementation of the corrective actions should be tested to see whether they are understood and are effective in addressing the problem. Management should continue to periodically review and test such corrective actions to see that they remain effective on a continuing basis.

The SANS (SysAdmin, Audit, Network, Security) Institute (or simply SANS) is one of the most trusted and largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. SANS was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

The "Top Ten" list was first released by the SANS Institute and the National Infrastructure Protection Center (NIPC) in 2000. Today, though it is now called the Top Twenty, it covers over 230 well-known, often-exploited vulnerabilities in the Windows and UNIX environments. Thousands of organizations use the list to prioritize their efforts so they can close the most dangerous holes first. The majority of successful attacks on computer systems via the Internet can be traced to the exploitation of security flaws on this list. The SANS/FBI Top Twenty includes step-by-step instructions and pointers to additional information useful for correcting the flaws. SANS updates the list and the instructions as more critical threats and more current or convenient methods are identified.

The SANS Institute states that the SANS Top-20 2004 is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited elements in UNIX (SUN Solaris, IBM AIX, HP-UX, BSD, and Linux, etc.) environments. There are thousands of security incidents each year affecting these operating systems; however, the overwhelming majority of successful attacks target one or more of these twenty vulnerable services.

7.3 Risks of Non-compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

According to SANS, the vast majority of worms, trojan horses, viruses, and other successful cyber attacks are made possible by vulnerabilities in a small number of common operating system services. Attackers are opportunistic and will take the easiest and most convenient route to exploit known flaws with the most effective and widely available attack tools. They count on organizations not applying operating system patches or correcting the problems, attacking indiscriminately, compromising any Internet connected vulnerable system. The easy and

destructive spread of worms, such as nimda, Blaster, Slammer, and Code Red, can be traced directly to exploitation of unpatched vulnerabilities.

The FISCAM states that the "inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure and modification of data".

The following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- *By obtaining direct access to **data files**, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) inadvertently or purposefully change a receivable balance, or (4) obtain confidential information about business transactions or individuals.*

- *By obtaining access to **application programs** used to process transactions, an individual could make unauthorized changes to these programs or introduce malicious programs, which in turn could be used to access data files, resulting in situations similar to those describe above, or to process unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for himself or herself.*

- *By obtaining access to **computer facilities** and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.*

The importance of having a comprehensive vulnerability testing program is highlighted by the following examples:

- *Following a major failure, systems can be brought back online quickly by re-installation from the original or backup copies of the software. But in some cases, patches and security hotfixes are not included in the original or backup copies of the software. As a result, the system can be restored to operation, but in a vulnerable unpatched condition. Since the system was previously originally patched, its vulnerable condition may go unnoticed. This re-enforces the importance of comprehensive testing to include "known" patched systems.*

- *Some software installs various services by default which could be unneeded, not apparent to the installer, and vulnerable.*

- *Many new vulnerabilities are discovered in existing software each month. It would be extremely difficult for system administrators to manually track new vulnerabilities and determine applicability to their systems. Most vulnerability scanning software is supported by its original vendor and continually updated with signatures for newly discovered vulnerabilities.*

7.4 Specific Controls to be Implemented

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The SANS Top-20 list is a living document and is regularly updated. It includes step-by-step instructions and pointers to additional information useful for correcting common security flaws in Windows and UNIX operating systems. SANS updates the list and the instructions as more critical threats and more current or convenient methods of protection are identified. Table E-18 provides a list of the 20 vulnerabilities as described by the SANS Institution.

Table E-17. SANS Top 20 Internet Security Vulnerabilities (as of 10/08/04 – v. 5)

Top Vulnerabilities to Windows Systems
W1 - Web Servers & Services
W2 - Workstation Service
W3 - Windows Remote Access Services
W4 - Microsoft SQL Server (MSSQL)
W5 - Windows Authentication
W6 - Web Browsers
W7 - File-Sharing Applications
W8 - LSAS Exposures
W9 - Mail Client
W10 - Instant Messaging
Top Vulnerabilities to UNIX Systems
U1 - BIND Domain Name Service (DNS)
U2 - Web Server
U3 - Authentication
U4 - Version Control Systems
U5 - Mail Transport Service
U6 - Simple Network Management Protocol (SNMP)
U7 - Open Secure Sockets Layer (SSL)
U8 - Misconfiguration of Enterprise Services NIS/NFS
U9 - Databases
U10 - Kernel

For each of the vulnerabilities, SANS lists on its website: description, operating system affected, related CVE entries, how to protect against the vulnerability, and how to test to determine if the vulnerability exists on a system. For the testing process for each vulnerability SANS indicates the manual process for testing (if any) as well as examples of automated tools (both open source and commercial) which can scan for the vulnerability.

NIST Special Publication 800-42, Guideline on Network Security Testing, identifies several different types of security testing and vulnerability monitoring. Some testing techniques are predominantly manual, requiring an individual to initiate and conduct the test. Other tests are

highly automated and require less human involvement. Regardless of the type of testing, staff that setup and conduct security testing should have significant security and networking knowledge, including significant expertise in the following areas: network security, firewalls, intrusion detection systems, operating systems, programming and networking protocols (such as TCP/IP).

The following are types of testing techniques and tools:

- *Network Scanning*
- *Vulnerability Scanning*
- *Password Cracking*
- *Log Review*
- *Integrity Checkers*
- *Virus Detection*
- *War Dialing*
- *War Driving (802.11 or wireless LAN testing)*
- *Penetration Testing*

NIST SP 800-42 also references the SANS Top 20 Internet Security Vulnerabilities in its discussion and recommendations regarding security testing. NIST specifically states that the main focus of this document is the basic information about techniques and tools for individuals to begin a network security testing program. But it also states that this document is by no means all-inclusive. Individuals and organizations should consult the references provided in this document, such as the SANS list, as well as vendor product descriptions and other sources of information. And although the document is not all-inclusive, it is comprehensive in that it discusses how to implement security testing for vulnerabilities such as the SANS list while keeping a perspective of aligning with other security related practices for government information systems (such as the System Development Life Cycle and Certification and Accreditation processes).

The BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All controls documented in the BPSSM are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, ***unless other compensatory controls are in place, which satisfy the control objective.***

Tables E-19 and E-20 list the controls in FISCAM and NIST SP 800-53 respectively which are applicable to ***a Testing Process for the SANS Top 20 Internet Security Vulnerabilities****. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-19. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-20.*

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in

Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-20 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to ***Testing for the SANS Top 20 Internet Security Vulnerabilities****. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.*

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-20 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-20, the corresponding FISCAM control in Table E-19, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines related to ***Testing for the SANS Top 20 Internet Security Vulnerabilities.***

7.5 Sample Instances of Lack of Identification and Remediation of Security Vulnerabilities and Recommended Testing Approaches

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Table E-19 below provides a listing of sample instances of lack of identification and remediation of the ***SANS Top 20 Internet Security Vulnerabilities*** *based on prior controls reviews and audits. Specifically, the table lists sample findings as identified in prior external audit(s), and the applicable SANS Internet Security Vulnerability and testing method for the selected cases as recommended by the SANS organization. The findings in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the testing recommendation listed for*

each issue is taken from the SANS Institute publication and website SANS Top 20 Internet Security Vulnerabilities. Some of the testing recommendations are for specific applications or operating systems, but are not written to take into account the business operations and technology environment of specific CMS sites.

Table E-18. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	*Applicable SANS Internet Security Vulnerability*	*SANS Recommended Testing Method*
Weak, default, or expired passwords were detected on systems, increasing the risk that a malicious user could gain unauthorized access to system resources and data. [Note: this finding was specific to a Windows operating system installation.]	*W5 - Windows Authentication*	*Although there are observable symptoms of general password weakness, such as the existence of active accounts for users who have departed the organization or services which are not running, the only way to know for certain that each individual password is strong is to test all of them against the same password cracking tools used by attackers.* *Please Note: Password scanners should never be run, even on administered systems, without explicit and preferably written permission from organization management.* *View the Local Security Policy to determine settings for complexity requirements. Also view settings for: Enforce password history, Maximum password age, Minimum password age, Minimum password length, and Store password using reversible encryption.*
Services vulnerable to buffer overflow attacks are present and unpatched on the servers, increasing the risk that systems will be compromised by malicious users. [Note: this finding was specific to a Windows operating system installation.]	*W1 - Web Servers & Services*	*Any default or unpatched web server installations should be presumed vulnerable. Also check any web server and associated service's patch and software revision levels, including configurations, against the vendor-supplied security information and the CVE database on a regular basis to assess potential vulnerability. It is important to realize that new issues are discovered regularly and it is best practice to consult to make good use of the Windows Update website, Microsoft Security Baseline Analyzer and Automatic Updates feature to properly assess and eliminate potential vulnerabilities.*

Finding	*Applicable SANS Internet Security Vulnerability*	*SANS Recommended Testing Method*
Outdated versions of Sendmail and Apache and unpatched versions of SSH, FTP and Oracle leaves the servers vulnerable to known vulnerabilities.	*U5 - Mail Transport Service*	*Sendmail has had a large number of vulnerabilities in the past. These vulnerabilities have often been due to its complexity. These have made Sendmail one of the most exploited services on the Internet.* *Any outdated or unpatched version of the software is likely to be vulnerable.* *To determine the version of Sendmail, use the following command:* *echo \$Z | sendmail -bt -d* *[The version string returned by the daemon should not always be trusted as it is just read from a text file on the system that may not have been updated properly.]* *To determine whether the running version is current, check the current release of Sendmail versions at the Sendmail internet homepage.*
	U9 - Databases	*Ensure that all DBMS that come with an operating system are running the latest version. Unpatched or outdated versions of databases are likely to be vulnerable. Default installations of DBMS are likely to have vulnerabilities that could be exploited by an attacker* *Perform a vulnerability scan on systems to determine whether DBMS software is vulnerable.*
Users or shares were identified using a null session. A null session is a NetBIOS connection established with a zero length string as user, password, and domain name, which is designed to enable enumeration of shares and users. This capability has always been present in Windows NT, but was discovered to allow access to the registry with the same level of permissions as the Everyone group	*W3 - Windows Remote Access Services*	*NETBIOS related issues:* *For Windows NT (SP4), Windows 2000, Windows XP, and Windows 2003, the Microsoft Baseline Security Analyzer will report hosts that are vulnerable to SMB exploits and may be used to fix the problem. The tests can be run locally or on remote hosts.* *Windows NT, Windows 2000, Windows*

Finding	*Applicable SANS Internet Security Vulnerability*	*SANS Recommended Testing Method*
and allows users and shares to be enumerated by anonymous users.		*XP, and Windows 2003 users can simply type 'net share' from the command prompt to see what resources are being shared. For more information about the 'net share' command, type 'net share /?'* ***IMPORTANT NOTE:** Before modifying any shared resource, make sure that it is understood how to restore the resource if a problem occurs. It is recommended that any modifications are thoroughly tested before implementation in a production environment. For information about shared resources, view the appropriate article in the Microsoft Knowledge Base section of the Microsoft website.* *Anonymous Logon related issues.* *Try to establish a null session to the computer by issuing the following command from the command prompt (Start --> Run --> type cmd):* *C:\>net use \\ipaddress\ipc$ "" /user:""* *The preceding syntax connects to the hidden interprocess communications "share (IPC$) at ipaddress (/user:"") with a null () password.* *If "The command completed successfully" is received, then the system is potentially vulnerable to remote interrogation and account enumeration.*

Finding	*Applicable SANS Internet Security Vulnerability*	*SANS Recommended Testing Method*
MssqlResolutionServiceBo: Microsoft SQL Server Resolution Service heap buffer overflow (CAN-2002-0729). *Microsoft SQL Server 2000 is vulnerable to a heap buffer overflow in the SQL Server Resolution Service, which is used to direct client requests to the proper port when multiple instances of the SQL Server are running on the same system. By sending a specially-crafted request to UDP port 1434 consisting of a byte set to 0x08 followed by an overly long string and a colon character (:), a remote attacker could overflow a buffer and cause the SQL Server service to crash or execute arbitrary code on the system with the same privileges as the SQL Server.*	*W4 - Microsoft SQL Server (MSSQL)*	*Microsoft has published a set of security tools at the Microsoft website. The toolkit named the SQL Critical Update Kit contains valuable tools such as SQL Scan, SQL Check, and SQL Critical Update.*
IeGopherBo: Microsoft Internet Explorer Gopher client malformed reply buffer overflow. *Microsoft Internet Explorer versions 5.01 through 6.0, Microsoft Proxy Server 2.0, and Microsoft Internet Security and Acceleration (ISA) Server 2000 are vulnerable to a buffer overflow in the built-in Gopher client. A remote attacker could exploit this vulnerability by creating a Web page or an HTML email that redirects a victim to a malicious Gopher server, which could be used to overflow a buffer in the code in Internet Explorer that handles Gopher replies. An attacker could use this vulnerability to execute arbitrary code and gain complete control of the victim's computer.*	*W6 - Web Browsers*	*If Internet Explorer is used on a system, there is no current way to know if it is vulnerable, due to the large number of unpatched vulnerabilities which exist. The Windows Update Site should be visited regularly and where possible the Automatic Updates feature enabled, ensuring that IE is protected from vulnerabilities that patches are available for. Users interested in further protection from browser vulnerabilities should consider employing a blend of the following recommendations:* *a. By far the most effective step towards a safe and secure browsing experience is to ensure the latest version of the web client is installed, which will feature new controls for heightened security and eliminate concerns identified in older versions of the application.* *b. Most Internet sites do not make use of ActiveX, but disabling this feature could*

Finding	Applicable SANS Internet Security Vulnerability	SANS Recommended Testing Method
		have adverse effects on other aspects of the system. Since the Windows Update web site, which uses ActiveX, would be adversely affected by this approach, try using the "Automatic Updates" features instead. c. A Best Practice recommendation is to not browse the web or access web resources when logged into the system with Administrator or high-level system privileges. d. If using an alternative browser is not an option, disabling ActiveX entirely should be considered except for internal ActiveX applets that can be preinstalled on the machine. Microsoft provides a way to stop an ActiveX control from running in Internet Explorer, and these controls are greatly enhanced for security in Windows XP SP2.
The rlogin service is enabled. The r-services, in conjunction with the /etc/hosts.equiv file and individual .rhosts files, place a system at risk. They allow users to log in or execute commands from a trusted system without re-authenticating.	U3 - Authentication	General Considerations Even if password hashes are protected by /etc/shadow or other implementations, passwords can be guessed by other means. There are other common areas of password weakness, including the existence of unused accounts for users that have departed an organization. Organizations are commonly negligent in closing down old user accounts unless there are procedures in place or the administrator is particularly diligent. Default installations (either from the manufacturer or by an administrator) of operating systems or network applications may introduce a wide range of unneeded and unused services. In many cases the uncertainty about operating system or application needs leads many manufacturers or administrators to install all of the software in case it is needed in the future. This simplifies the installation

Finding	Applicable SANS Internet Security Vulnerability	SANS Recommended Testing Method
		process significantly but also introduces a wide range of unneeded services and accounts that have default/weak/or known passwords. Additionally, passwords sent over the network in clear-text, such as through telnet, FTP or HTTP, are at risk of being sniffed by malicious individuals. The use of an encrypted connection, such as with OpenSSH or SSL, can be used to hide a password from anyone spying the network connection.
The Simple Mail Transport Protocol (SMTP) service appears to allow relaying. Mail servers should not allow relaying as this could allow the server to be used to falsify e-mails or send SPAM, potentially opening the organization up to liability.	U5 - Mail Transport Service	Check the server's relay status What is an open relay Relaying mail is the basic function of an MTA but erroneous configurations may turn your MTA into an open relay. This occurs when an MTA relays a mail message where neither the sender nor the recipient is a local user. In other words, the sender and the recipient are not part of the domain and the MTA is unrelated to the transaction. Under normal circumstances the email would have no reason for passing through the MTA. Checking if an MTA is an open relay Checking if an MTA is an open relay is one of the most important things to do after checking its patch level. This determines whether or not someone can send unsolicited commercial email (SPAM) through an MTA. Publicly available tools on the internet will assist in doing this. What is a Realtime Blackhole List? A Real-time Blackhole List (RBL) is a list of IP addresses of servers whose owners refuse to stop the proliferation of SPAM on the Internet. These lists are used by mail administrators in order to refuse connections to their MTAs coming from

Finding	Applicable SANS Internet Security Vulnerability	SANS Recommended Testing Method
		these know spammers. If an organization's mail server is on one of these lists, chances are it's an open relay unless its configuration has been recently modified. RBLs are publicly available on the internet.

7.6 Periodic Review and Testing of Controls

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems (which all CMS systems are considered to be). Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

Often, several of these testing techniques are used together to gain a more comprehensive assessment of the overall network security posture. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Some vulnerability scanners incorporate password

cracking. None of these tests by themselves will provide a complete picture of the network or its security posture.

NIST Special Publication 800-42 Guideline on Network Security Testing stresses the need for an effective security testing program within Federal agencies. Testing serves several purposes. One, no matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies coupled with vendor cost and schedule pressures, means that exploitable flaws will always be present or surface over time. Accordingly, security testing must fill the gap between the state of the art in system development and actual operation of these systems. Two, security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Aside from development of these systems, the operational and security demands must be met in a fast changing threat and vulnerability environment. Attempting to learn and repair the state of your security during a major attack is very expensive in cost and reputation, and is largely ineffective. Three, security testing is an essential component of improving the security posture of organizations. Organizations that have an organized, systematic, comprehensive, ongoing, and priority driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.

The BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

7.7 Conclusion

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The objective of an Information Security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process or store Medicare related data have some level of sensitivity and require protection. This protection should come not only in the form of applying general access controls but also the specific elimination of common information system security vulnerabilities, such as those identified in the SANS Top 20 Internet Security Vulnerabilities list.

The implementation of controls related to security testing should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management). Senior management's awareness, support, and involvement are essential in establishing the control environment needed to promote compliance with the entity's information security program. Top management should understand the entity's security risks and actively support and monitor the effectiveness of the entity's security policies. If senior management does not monitor the security program, it is unlikely that others in the organization will be committed to properly implementing it.

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-

going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table E-19. Applicable FISCAM Controls

FISCAM General Controls
SP-1 Periodically Assess Risks
SP-2 Document an entity-wide security program plan
SP-2.1 A security plan is documented and approved
SP-2.2 The plan is kept current
SP-3 Establish a security management structure and clearly assign security responsibilities
SP-3.2 Information security responsibilities are clearly assigned
SP-4 Implement effective security related personnel policies
SP-4.2 Employees have adequate training and expertise
AC-2 Maintain a current list of authorized users and their access authorized
AC-2.1 Resource owners have identified authorized users and their access authorized
AC-3 Establish physical and logical controls to prevent or detect unauthorized access
AC-3.1 Adequate physical security controls have been implemented
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access
AC-3.2 Adequate logical access controls have been implemented
A. Passwords, tokens, or other devices are used to identify and authenticate users
B. Identification of access paths
C. Logical controls over data files and software programs
D. Logical controls over a database
E. Logical controls over telecommunications access
AC-3.3 Cryptographic tools
AC-3.4 Sanitation of equipment and media prior to disposal or reuse
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action
AC-4.1 Audit trails are maintained
CC-2 Test and approve all new and revised software
CC-2.1 Changes are controlled as programs progress through testing to final approval
CC-2.2 Emergency changes are promptly tested and approved
CC-2.3 Distribution and implementation of new or revised software is controlled
CC-3 Control software libraries
CC-3.2 Access to program libraries is restricted
CC-3.3 Movement of programs and data among libraries is controlled
SS-1 Limit access to system software
SS-1.1 Access authorizations are appropriately limited
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths
SS-2 Monitor access to and use of system software
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities

FISCAM General Controls
SS-3 Control system software changes
SS-3.1 System software changes are authorized, tested and approved before implementation
SD-1 Segregate incompatible duties and establish related policies
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties
SD-2 Establish access controls to enforce segregation of duties
SD-2.1 Physical and logical access controls have been established
SD-3 Control personnel activities through formal operating procedures and supervision and review
SD-3.1 Formal procedures guide personnel in performing their duties
SD-3.2 Active supervision and review are provided for all personnel
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources
SC-1.1 Critical data and operations are identified and prioritized
SC-1.2 Resources supporting critical operations are identified
SC-4 Periodically test the contingency plan and adjust it as appropriate
SC-4.1 The plan is periodically tested
SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly

Table E-20. Applicable NIST SP 800-53 Controls

Corresponding FISCAM Control	NIST 800-53 Recommended Security Controls	
	Family: Access Control	
	AC-1	Access Control Policy and Procedures
AC-2, AC-3.2	AC-3	Access Enforcement
	AC-4	Information Flow Enforcement
AC-3.2, SD-1.2	AC-5	Separation of Duties
	Family: Awareness and Training	
	AT-3	Security Training
	Family: Certification, Accreditation, and Security Assessments	
SP-5.1	CA-2	Security Assessments
	CA-7	Continuous Monitoring
	Family: Configuration Management	
SS-3.2, CC-2.2	CM-3	Configuration Change Control
SS-3.1, SS-3.2, CC-2.1	CM-4	Monitoring Configuration Changes
	Family: Contingency Planning	
SC-3.1	CP-4	Contingency Plan Testing
	Family: Identification and Authentication	
	IA-1	Identification and Authentication Policy and Procedures
	Family: Maintenance	
	MA-1	System Maintenance Policy and Procedures
SS-3.1	MA-2	Periodic Maintenance

Corresponding FISCAM Control	*NIST 800-53 Recommended Security Controls*	
	MA-3	*Maintenance Tools*
SS-3.1	*MA-4*	*Remote Maintenance*
SC-1.2	*MA-6*	*Timely Maintenance*
	Family: Media Protection	
	MP-1	*Media Protection Policy and Procedures*
AC-3.1	*MP-4*	*Media Storage*
	MP-5	*Media Transport*
AC-3.4	*MP-6*	*Media Sanitization*
AC-3.4	*MP-7*	*Media Destruction and Disposal*
	Family: Physical and Environmental Protection Policy and Procedures	
	PE-1	*Physical and Environmental Protection Policy and Procedures*
AC-3.1	*PE-2*	*Physical Access Authorizations*
AC-3.1	*PE-3*	*Physical Access Control*
	Family: Planning	
	PL-1	*Security Planning Policy and Procedures*
SP-2.1	*PL-2*	*System Security Plan*
SP-2.1	*PL-3*	*System Security Plan Update*
	PL-4	*Rules of Behavior*
	Family: Personnel Security	
SP-4.1	*PS-6*	*Access Agreements*
SP-4.1	*PS-7*	*Third-Party Personnel Security*
	Family: Risk Assessment	
	RA-1	*Risk Assessment Policy and Procedures*
SP-1, AC-1.1, AC-1.2	*RA-2*	*Security Categorization*
SP-1	*RA-3*	*Risk Assessment*
SP-1	*RA-4*	*Risk Assessment Update*
	RA-5	*Vulnerability Scanning*
	Family: System and Services Acquisition	
CM-3	*SA-11*	*Developer Security Testing*
	Family: System and Information Integrity	
	SI-4	*Intrusion Detection Tools and Techniques*
SP.3.4	*SI-5*	*Security Alerts and Advisories*
SS-2.2	*SI-6*	*Security Functionality Verification*
	SI-7	*Software and Information Integrity*

8.0 References

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999.

OMB Guidance on FISMA Reporting Instructions, Memorandum for Heads of Executive Departments and Agencies, June 13, 2005.

Federal Information Security Management Act (FISMA) of 2002.

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.

Appendix F: - *Security Configuration Management*

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Table of Contents

1.0 Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government.

2.0 Security Technical implementation Guides (STIGs)

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The guidelines, called Security Technical Implementation Guides (STIG), and checklists, called Security Checklists, are developed to help system operators configure security within their systems to the highest level possible. The STIGs and Security Checklists were formerly available at a NIST web page because the source Defense Information Systems Agency (DISA) web page was restricted to users in .gov and .mil domains. That restriction is no longer in effect, so NIST no longer hosts the DISA STIG and Security Checklist links.

The DISA web page link for STIGs is: http://iase.disa.mil/stigs/stig/index.html, and for Security Checklists: http://iase.disa.mil/stigs/checklist/index.html. CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List located at: http://iase.disa.mil/stigs/index.html so they will be notified whenever updated or new STIGs become available.

The National Security Agency (NSA) has also developed and distributed configuration guidance for a wide variety of software from open-source to proprietary. The objective of the NSA configuration guidance program is to provide administrators with the best possible security options in the most widely used products. NSA provides these guidelines at: http://www.nsa.gov/snac/downloads_all.cfm.

The Center for Internet Security (CIS) provides security configuration benchmarks that represent a prudent level of due care, and are working to define consensus best-practice security configurations for computers connected to the Internet. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks. The CIS benchmarks and scoring tools are available for download at: http://www.cisecurity.com/benchmarks.html.

The use of STIGs will:

- *Reduce the likelihood of successful intrusions or attacks;*
- *Facilitate secure configuration of systems prior to network deployment; and*
- *Assist with monitoring systems for on-going conformance with security configurations.*

The latest versions of these documents can be obtained from the DISA web site by subscribing to the STIG-News Mailing List to receive update notifications.

3.0 Department of Health and Human Services Minimum Security Configuration Standards

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

The Department of Health and Human Services (HHS) is responsible for implementing and administering an information assurance and privacy program to protect its information resources, in compliance with applicable public laws, federal regulations, and Executive Orders, including the Federal Information Security Management Act of 2002 (FISMA); the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, dated November 28, 2000; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HHS Minimum Security Configuration Standards were created as part of the HHS Information Assurance and Privacy Program to supply standards for configuring Departmental Systems and Applications using Minimum Standard Configurations.

At a minimum, CMS expects compliance with the HHS configuration standards described below.

Table F-1. Windows 2000 Server Configuration Guide

Category	*800-53*	*Map*	*Action*
Access Controls	*Access Enforcement*	*AC-3*	*Only allow Server Administrators to Schedule Tasks*
Access Controls	*Access Enforcement*	*AC-3*	*Do Not Allow Automatic Administrative Logon*
Access Controls	*Access Enforcement*	*AC-3*	*Configure all disk volumes to use the NTFS file system*
Access Controls	*Access Enforcement*	*AC-3*	*Set Unsigned Driver Installation Behavior To "Warn but allow installation" or "Do not allow installation"*
Accounts	*Account Management*	*AC-2*	*Rename Administrator Account*

Category	800-53	Map	Action
Accounts	Account Management	AC-2	Rename and disable the Guest Account
Accounts	User Identification and Authentication	AC-3 AC-7 IA-2 IA-5	Configure the system per 800-53 Account Policy Control Requirements
Audit	Auditable Events	AU-2 AU-4 AU-5	Configure the system per 800-53 Audit Control Requirements
Logon	User Identification and Authentication	IA-2	Configure the system to use an HHS accepted warning banner.
Logon	User Identification and Authentication	IA-2	Do Not Allow System to be Shut Down Without Having to Log On
Logon	User Identification and Authentication	IA-2	Enable CTRL+ALT+Delete Requirement for Logon
Media	Remote Access	AC-17	Restrict CD-ROM Access to Administrators
Media	Remote Access	AC-17	Restrict Floppy Access to Administrators
Network Access	Remote Access	AC-17	Digitally Encrypt Secure Channel Data
Network Access	Remote Access	AC-17	Digitally Sign Client Communication
Network Access	Remote Access	AC-17	Digitally Sign Secure Channel Data
Network Access	Remote Access	AC-17	Digitally Sign Server Communication
Network Access	Remote Access	AC-17	Disable Dial-in access to the server unless required for the server role
Network Access	Remote Access	AC-17	Disable Sending Unencrypted Password to Connect to Third-Party SMB Servers
Network Access	Remote Access	AC-17	Require Strong (Windows 2000 or later) Session Key
Network Access	Remote Access	AC-17	Set LAN Manager Authentication Level to use NTLMv2
Password Management	Access Enforcement	AC-3	Do Not Store Passwords Using Reversible Encryption
Password Management	Authenticator Management	IA-5	Do Not Display Last User Name in Logon Screen
Patches	Flaw Remediation	SI-2	Apply critical Operating System security patches
Patches	Flaw Remediation	SI-2	Ensure That Before the System is Loaded Onto an Operational Network, Security Patches,

Category	800-53	Map	Action
			Service Packs, And Hot Fixes are all Tested
Permissions	Access Enforcement	AC-3	Configure the system per 800-53 Access Enforcement Control Requirements for files/folders.
Permissions	Access Enforcement	AC-3	Configure the system per 800-53 Access Enforcement Control Requirements for registry keys.
Registry Permission	Least Functionality	CM-7	Disable Automatic Execution of the System Debugger
Registry Permission	Least Functionality	CM-7	Disable automatic reboots after a Blue Screen of Death
Registry Permission	Least Functionality	CM-7	Disable autoplay for new/current users
Registry Permission	Least Functionality	CM-7	Disable autoplay from any disk type, regardless of application
Registry Permission	Least Functionality	CM-7	Remove administrative shares on servers
Registry Permission	User Identification and Authentication	IA-2	Disable Automatic Logon
Registry Permission	Information Remnants	SC-4	Suppress Dr. Watson Crash Dumps
Registry Permission	Denial of Service Protection	SC-5	Configure the system per 800-53 Denial of Service Control Requirements
Service	Least Functionality	CM-7	Configure permissions for the following services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause.' Alerter Automatic Updates Background Intelligent Transfer Service (a.k.a. BITS) Clipbook Computer Browser Fax Service FTP Publishing Service IIS Admin Service Internet Connection Sharing Messenger NetMeeting Remote Desktop Sharing Remote Registry Service Routing and Remote Access Simple Mail Transfer Protocol

Category	800-53	Map	Action
			(SMTP) *Simple Network Management Protocol (SNMP) Service* *Simple Network Management Protocol (SNMP) Trap* *Telnet* *World Wide Web Publishing Services*
Smart Cards	*User Identification and Authentication*	*IA-2*	*Configure Smart Card Removal Behavior*
User Rights	*Access Enforcement*	*AC-3* *AU-8* *AU-9*	*Audit user rights assignments to ensure they are appropriately applied*

Table F-2. Windows 2003 Server Configuration Guide

Category	*800-53*	*Map*	*Action*
Access Controls	*Access Enforcement*	*AC-3*	*Only allow Server Administrators to Schedule Tasks*
Access Controls	*Access Enforcement*	*AC-3*	*Do Not Allow Automatic Administrative Logon*
Access Controls	*Access Enforcement*	*AC-3*	*Configure all disk volumes to use the NTFS file system*
Access Controls	*Access Enforcement*	*AC-3*	*Set Unsigned Driver Installation Behavior To "Warn but allow installation" or "Do not allow installation"*
Accounts	*Account Management*	*AC-2*	*Rename and enable Administrator Account*
Accounts	*Account Management*	*AC-2*	*Rename and disable the Guest Account*
Accounts	*User Identification and Authentication*	*AC-3 AC-7 IA-2 IA-5*	*Configure the system per 800-53 Account Policy Control Requirements*
Accounts	*Account Management*	*AC-2*	*Do not allow anonymous enumeration of SAM accounts*
Accounts	*Account Management*	*AC-2*	*Do not allow anonymous enumeration of SAM accounts and shares*
Accounts	*Account Management*	*AC-2*	*Disable anonymous SID/Name translation*
Accounts	*Account Management*	*AC-2*	*Limit local account use of blank passwords to console logon only*
Audit	*Auditable Events*	*AU-2 AU-4 AU-5*	*Configure the system per 800-53 Audit Control Requirements*
Device	*Session Lock*	*AC-11*	*Disable allowing users undock without having to log on*
Logon	*User Identification and Authentication*	*IA-2*	*Configure the system to use an HHS accepted warning banner.*
Logon	*User Identification and Authentication*	*IA-2*	*Do Not Allow System to be Shut Down Without Having to Log On*
Logon	*User Identification and Authentication*	*IA-2*	*Enable CTRL+ALT+Delete Requirement for Logon*
Media	*Remote Access*	*AC-17*	*Restrict CD-ROM Access to Locally Logged-On User Only*
Media	*Remote Access*	*AC-17*	*Restrict Floppy Access to Locally Logged-On User Only*
Network Access	*Account Management*	*AC-2*	*Disable letting Everyone permissions apply to anonymous*

Category	800-53	Map	Action
			users
Network Access	Account Management	AC-2	Configure the sharing and security model for local accounts to Classic (Local users authenticate as themselves)
Network Access	Remote Access	AC-17	Digitally Encrypt Secure Channel Data
Network Access	Remote Access	AC-17	Digitally Sign Client Communication
Network Access	Remote Access	AC-17	Digitally Sign Secure Channel Data
Network Access	Remote Access	AC-17	Digitally Sign Server Communication
Network Access	Remote Access	AC-17	Require Strong (Windows 2000 or later) Session Key
Network Access	Remote Access	AC-17	Disable Sending Unencrypted Password to Connect to Third-Party SMB Servers
Network Access	Remote Access	AC-17	Restrict anonymous access to Named Pipes and Shares
Network Access	Remote Access	AC-17	Configure system so that no shares can be accessed anonymously
Network Access	Transmission Integrity	SC-8	Do not allow storage of credentials or .NET passports for network authentication
Network Security	Information Remnants	SC-4	Do not store LAN Manager password hash value on next password change
Network Security	User Identification and Authentication	IA-2	Configure LAN Manager Authentication Level to "Send NTLMv2 response only\refuse LM"
Password Management	Access Enforcement	AC-3	Do Not Store Passwords Using Reversible Encryption
Password Management	Authenticator Management	IA-5	Do Not Display Last User Name in Logon Screen
Password Management	Authenticator Management	IA-5	Disable System Maintenance of Computer Account Password (Domain Controllers)
Patches	Flaw Remediation	SI-2	Apply critical Operating System security patches
Patches	Flaw Remediation	SI-2	Ensure That Before the System is Loaded Onto an Operational Network, Security Patches, Service Packs, And Hot Fixes

Category	800-53	Map	Action
			are all Tested
Permissions	Access Enforcement	AC-3	Configure the system per 800-53 Access Enforcement Control Requirements for files/folders.
Permissions	Access Enforcement	AC-3	Configure the system per 800-53 Access Enforcement Control Requirements for registry keys.
Registry Permission	Denial of Service Protection	SC-5	Configure the system per 800-53 Denial of Service / Network Security Control Requirements
Service	Least Functionality	CM-7	Configure permissions for the following services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause.' Alerter (Alerter) Client Service for NetWare (NWCWorkstation) Clipbook (ClipSrv) Fax Service (Fax) File Replication (NtFrs) File Server for Macintosh (MacFile) FTP Publishing Service (MSFtpsvc) Help and Support (helpsvc) HTTP SSL (HTTPFilter) IIS Admin Service (IISADMIN) Indexing Service (cisvc) License Logging Service (LicenseService) Messenger (Messenger) Microsoft POP3 Service NetMeeting Remote Desktop Sharing (mnmsrvc) Network Connections Network News Transport Protocol (NNTP) (NntpSvc) Print Server for Macintosh (MacPrint) Print Spooler (Spooler) Remote Access Auto Connection Manager (RasAuto) Remote Access Connection Manager (RasMan) Remote Administration Service

Category	800-53	Map	Action
			Remote Desktop Help Session Manager (RDSessMgr) *Remote Installation (BINLSVC)* *Remote Procedure Call (RPC) Locator (RpcLocator)* *Remote Registry Service (RemoteRegistry)* *Remote Server Manager (AppMgr)* *Remote Server Monitor (Appmon)* *Remote Storage Notification (Remote_Storage_User_Link)* *Remote Storage Server (Remote_Storage_Server)* *Simple Mail Transfer Protocol (SMTP) (SMTPSVC)* *SNMP Service (SNMP)* *SNMP Trap Service (SNMPTRAP)* *Telephony (TapiSrv)* *Telnet (TlntSvr)* *Terminal Services (TermService)* *Trivial FTP Daemon (tftpd)* *Wireless Configuration (WZCSVC)* *World Wide Web Publishing Services (W3SVC)*
Service	*Least Functionality*	*CM-7*	*Review all services for proper configuration and disable unneeded services*
Registry Permission	*Least Functionality*	*CM-7*	*Remove administrative shares on servers*
User Rights	*Access Enforcement*	*AC-3* *AU-8* *AU-9*	*Audit user rights assignments to ensure they are appropriately applied*

Table F-3. Windows 2000 Professional Configuration Guide

Category	800-53	Map	Action
Access Controls	Access Enforcement	AC-3	Do Not Allow Automatic Administrative Logon
Access Controls	Access Enforcement	AC-3	Configure all disk volumes to use the NTFS file system
Access Controls	Access Enforcement	AC-3	Enable account lockout after a specific amount of time
Access Controls	Access Enforcement	AC-3	Set Unsigned Driver Installation Behavior To "Warn but allow installation" or "Do not allow installation"
Accounts	Account Management	AC-2	Rename Administrator Account
Accounts	Account Management	AC-2	Rename and disable the Guest Account
Accounts	User Identification and Authentication	AC-3 AC-7 IA-2 IA-5	Configure the system per 800-53 Account Policy Control Requirements
Audit	Auditable Events	AU-2 AU-4 AU-5	Configure the system per 800-53 Audit Control Requirements
Logon	User Identification and Authentication	IA-2	Configure the system to use an HHS accepted warning banner.
Logon	User Identification and Authentication	IA-2	Do Not Allow System to be Shut Down Without Having to Log On
Logon	User Identification and Authentication	IA-2	Enable CTRL+ALT+Delete Requirement for Logon
Media	Remote Access	AC-17	Restrict CD-ROM Access to Locally Logged-On User Only
Media	Remote Access	AC-17	Restrict Floppy Access to Locally Logged-On User Only
Network Access	Remote Access	AC-17	Digitally Encrypt Secure Channel Data
Network Access	Remote Access	AC-17	Digitally Sign Client Communication
Network Access	Remote Access	AC-17	Digitally Sign Secure Channel Data
Network Access	Remote Access	AC-17	Digitally Sign Server Communication
Password Management	Authenticator Management	IA-5	Do Not Display Last User Name in Logon Screen
Password Management	Authenticator Management	IA-5	Domain Members: Disable machine account password changes
Patches	Flaw Remediation	SI-2	Service Pack and Security

Category	800-53	Map	Action
			Updates Test all software and patch updates Install all Major Service Packs and Security Updates Install all critical security updates as issued by the software developer
Registry Permission	Least Functionality	CM-7	Disable CD Autorun
Registry Permission	User Identification and Authentication	IA-2	Disable Automatic Logon
Service	Least Functionality	CM-7	Configure permissions for the following services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause.' Alerter Clipbook Computer Browser Fax Service FTP Publishing Service IIS Admin Service Indexing Service Messenger Net Logon Network DDE Share Database Manager Network Dynamic Data Exchange (DDE) Remote Desktop Help Session Manager Remote Registry Service Routing and Remote Access Simple Mail Transfer Protocol (SMTP) Simple Network Management Protocol (SNMP) Service Simple Network Management Protocol (SNMP) Trap SSDP Discovery Service Task Scheduler Telnet Terminal Services Universal Plug and Play Device Host

Category	800-53	Map	Action
			World Wide Web Publishing Services
Service	Least Functionality	CM-7	Disable all services that do not directly support the role of the workstation
Accounts	Account Management	AC-2	Do not allow anonymous enumeration of SAM accounts
Accounts	Account Management	AC-2	Do not allow anonymous enumeration of SAM shares
Accounts	Account Management	AC-2	Disable anonymous SID/Name translation
Device	Least Functionality	CM-7	Disable unused networking interfaces
Device	Session Lock	AC-11	Disable allowing users undock without having to log on
Logon	System Use Notification	AC-8	Set Message Text for Users Attempting to Log On
Network Access	Account Management	AC-2	Disable letting Everyone permissions apply to anonymous users
Network Access	Account Management	AC-2	Configure the sharing and security model for local accounts to Classic (Local users authenticate as themselves)
Network Access	Remote Access	AC-17	Restrict anonymous access to Named Pipes and Shares
Network Access	Remote Access	AC-17	Disable Dial-in access to the workstation
Network Access	Remote Access	AC-17	Require Strong (Windows 2000 or later) Session Key
Network Access	Transmission Integrity	SC-8	Do not allow storage of credentials or .NET passports for network authentication
Network Security	Authenticator Management	IA-5	Configure LDAP client signing requirements to Negotiate Signing
Network Security	Information Remnants	SC-4	Do not store LAN Manager password hash value on next password change
Network Security	User Identification and Authentication	IA-2	Configure LAN Manager Authentication Level to "Send NTLMv2 response only\refuse LM"
Password Management	Access Enforcement	AC-3	Do Not Store Passwords Using Reversible Encryption
Password	Authenticator	IA-5	Prevent System Maintenance of

Category	800-53	Map	Action
Management	Management		Computer Account Password
Patches	Flaw Remediation	SI-2	Apply critical Operating System security patches
Permissions	Access Enforcement	AC-3	Configure the system per 800-53 Access Enforcement Control Requirements for files/folders.
Permissions	Access Enforcement	AC-3	Configure the system per 800-53 Access Enforcement Control Requirements for registry keys.
Registry Permission	Least Functionality	CM-7	Disable Automatic Execution of the System Debugger
Registry Permission	Least Functionality	CM-7	Disable automatic reboots after a Blue Screen of Death
Registry Permission	Least Functionality	CM-7	Disable autoplay for new/current users
Registry Permission	Information Remnants	SC-4	Disable Dr. Watson Crash Dumps
Registry Permission	Denial of Service Protection	SC-5	Configure the system per 800-53 Denial of Service Control Requirements
Restricted Users	Access Enforcement	AC-3	Remove all Power Users, add as needed
User Rights	Access Enforcement	AC-3 AU-8 AU-9	Audit user rights assignments to ensure they are appropriately applied

Table F-4. Windows XP Professional Configuration Guide

Category	800-53	Map	Action
Access Controls	*Access Enforcement*	*AC-3*	*Do Not Allow Automatic Administrative Logon*
Access Controls	*Access Enforcement*	*AC-3*	*Configure all disk volumes to use the NTFS file system*
Access Controls	*Access Enforcement*	*AC-3*	*Enable account lockout after specific length of time*
Access Controls	*Access Enforcement*	*AC-3*	*Set Unsigned Driver Installation Behavior To "Warn but allow installation" or "Do not allow installation"*
Accounts	*Account Management*	*AC-2*	*Rename Administrator Account*
Accounts	*Account Management*	*AC-2*	*Rename and disable the Guest Account*
Accounts	*User Identification and Authentication*	*AC-3 AC-7 IA-2 IA-5*	*Configure the system per 800-53 Account Policy Control Requirements*
Audit	*Auditable Events*	*AU-2 AU-4 AU-5*	*Configure the system per 800-53 Audit Control Requirements*
Logon	*User Identification and Authentication*	*IA-2*	*Configure the system to use an HHS accepted warning banner.*
Logon	*User Identification and Authentication*	*IA-2*	*Do Not Allow System to be Shut Down Without Having to Log On*
Logon	*User Identification and Authentication*	*IA-2*	*Enable CTRL+ALT+Delete Requirement for Logon*
Media	*Remote Access*	*AC-17*	*Restrict CD-ROM Access to Locally Logged-On User Only*
Media	*Remote Access*	*AC-17*	*Restrict Floppy Access to Locally Logged-On User Only*
Network Access	*Remote Access*	*AC-17*	*Digitally Encrypt Secure Channel Data*
Network Access	*Remote Access*	*AC-17*	*Digitally Sign Client Communication*
Network Access	*Remote Access*	*AC-17*	*Digitally Sign Secure Channel Data*
Network Access	*Remote Access*	*AC-17*	*Digitally Sign Server Communication*
Network Access	*Remote Access*	*AC-17*	*Disable Sending Unencrypted Password to Connect to Third-Party SMB Servers*
Password Management	*Authenticator Management*	*IA-5*	*Do Not Display Last User Name*

Category	800-53	Map	Action
Password Management	Authenticator Management	IA-5	Mask password text fields
Password Management	Authenticator Management	IA-5	Domain Members: Disable Machine Account Password Changes
Patches	Flaw Remediation	SI-2	Service Packs and Security Updates Test all software and patch updates Install all Major Service Packs and Security Updates Install all critical security updates as issued by the software developer
Registry Permission	Least Functionality	CM-7	Disable automatic execution of CD applications
Registry Permission	Least Functionality	CM-7	Disable CD Autorun
Registry Permission	User Identification and Authentication	IA-2	Disable Automatic Logon
Service	Least Functionality	CM-7	Configure permissions for the following services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause.' Alerter Clipbook Computer Browser Fax Service FTP Publishing Service IIS Admin Service Indexing Service Messenger Net Logon NetMeeting Remote Desktop Sharing Network DDE Share Database Manager Network Dynamic Data Exchange (DDE) Remote Desktop Help Session Manager Remote Registry Service Routing and Remote Access Simple Mail Transfer Protocol (SMTP)

Category	800-53	Map	Action
			Simple Network Management Protocol (SNMP) Service *Simple Network Management Protocol (SNMP) Trap* *SSDP Discovery Service* *Task Scheduler* *Telnet* *Terminal Services* *Universal Plug and Play Device Host* *World Wide Web Publishing Services*
Service	*Least Functionality*	*CM-7*	*Disable all services that do not directly support the role of the workstation*

Table F-5. Windows NT Configuration Guide

Category	*800-53*	*Map*	*Action*
Access Controls	*Access Enforcement*	*AC-3*	*Configure all disk volumes to use the NTFS file system*
Access Controls	*Access Enforcement*	*AC-3*	*Restrict print driver installation to administrators.*
Accounts	*Account Management*	*AC-2*	*Disable the Null User account*
Accounts	*Account Management*	*AC-2*	*Rename Administrator Account*
Accounts	*Account Management*	*AC-2*	*Rename and disable the Guest Account*
Accounts	*User Identification and Authentication*	*AC-3* *AC-7* *IA-2* *IA-5*	*Configure the system per 800-53 Account Policy Control Requirements*
Audit	*Auditable Events*	*AU-2* *AU-4* *AU-5*	*Configure the system per 800-53 Audit Control Requirements*
Logon	*User Identification and Authentication*	*IA-2*	*Do Not Allow System to be Shut Down Without Having to Log On*
Logon	*User Identification and Authentication*	*IA-2*	*Configure the system to use an HHS accepted warning banner.*
Network Access	*Remote Access*	*AC-17*	*Configure the system to use NTLM v2 authentication to protect authenticator with encryption.*
Registry Permission	*User Identification and Authentication*	*IA-2*	*Disable Automatic Logon*
User Rights	*Access Enforcement*	*AC-3* *AU-8* *AU-9*	*Audit user rights assignments to ensure they are appropriately applied*

Table F-6. Solaris Configuration Guide

Category	800-53	Map	Action
Accounts / Access	Account Management	AC-2	Lock system accounts to prevent them from being used to log in to the system
Accounts / Access	Account Management	AC-2	No '.' (current working directory) or group/world writable files exist in root's $PATH.
Accounts / Access	Account Management	AC-2	Configure the system per 800-53 Account Policy Control Requirements.
Accounts / Access	Account Management	AC-2	Install TCP Wrappers
Accounts / Access	Account Management	AC-2	No '.' or group/world-writable directory in root $PATH
Accounts / Access	Account Management	AC-2	No user dot-files should be group/world writable
Accounts / Access	Account Management	AC-2	Remove user .netrc files
Accounts / Access	Account Management	AC-2	Set "mesg n" as default for all users
Accounts / Access	Account Management	AC-2	Set default group for root account
Accounts / Access	Account Management	AC-2	Set default UMASK for users, directories, and files to meet the needs of the system
Accounts / Access	Account Management	AC-2	Verify no legacy '+' entries exist in password, shadow, and group files
Accounts / Access	Account Management	AC-2	Verify that no UID 0 accounts exist other than root
Accounts / Access	Access Enforcement	AC-3	Add 'logging' option to root file system
Accounts / Access	Access Enforcement	AC-3	Add 'nosuid' option to /etc/rmmount.conf
Accounts / Access	Access Enforcement	AC-3	Create /etc[/ftpd]/ftpusers
Accounts / Access	Access Enforcement	AC-3	Disable "nobody" access for secure RPC
Accounts / Access	Access Enforcement	AC-3	Disable XDMCP port
Accounts / Access	Access Enforcement	AC-3	Prevent Syslog from accepting messages from network (except for Central Log Server)
Accounts / Access	Access	AC-3	Remove rhosts support in pam

Category	800-53	Map	Action
	Enforcement		
Accounts / Access	Access Enforcement	AC-3	Remove empty crontab files and restrict file permissions to authorized users
Accounts / Access	Access Enforcement	AC-3	Restrict at/cron to authorized users
Accounts / Access	Access Enforcement	AC-3	Restrict root logins to system console
Accounts / Access	Access Enforcement	AC-3	Run fix-modes
Accounts / Access	Access Enforcement	AC-3	Set default locking screensaver timeout
Accounts / Access	Access Enforcement	AC-3	Set EEPROM security-mode and log failed access
Accounts / Access	Access Enforcement	AC-3	Disable or configure the sadmind service to use strong authentication
Accounts / Access	System Use Notification	AC-8	Change default greeting string for Sendmail
Accounts / Access	System Use Notification	AC-8	Create warnings for FTP daemon
Accounts / Access	System Use Notification	AC-8	Create warnings for GUI-based logins
Accounts / Access	System Use Notification	AC-8	Create warnings for telnet daemon (if telnet is being used)
Auditing	Auditable Events	AU-2	Configure the system per 800-53 Audit Control Requirements.
Logon	User Identification and Authentication	IA-2	Configure the system to use an HHS accepted warning banner.
Installation / Patches	Transmission Integrity	SC-8	Utilize Secure Shell (SSH) for remote logins and file transfers.
Installation / Patches	Flaw Remediation	SI-2	Install SSH
Patches	Flaw Remediation	SI-2	Apply critical Operating System security patches
Patches	Flaw Remediation	SI-2	Ensure That Before the System is Loaded Onto an Operational Network, Security Patches, Service Packs, And Hot Fixes are all Tested
Misc / Tuning	Information Flow Enforcement	AC-4	Enable stack protection
Misc / Tuning	Information Flow Enforcement	AC-4	Restrict core dumps to protected directory
Misc / Tuning	Information Flow Enforcement	AC-4	Use better TCP sequence numbers

Category	800-53	Map	Action
Auditing	Protection of Audit Information	AU-9	Prevent the system from accepting syslog messages from the network.
Services	Least Functionality	CM-7	Disable X-Windows
Misc / Tuning	Least Functionality	CM-7	Configure the system per 800-53 File Permissions/Access Control Requirements.
Misc / Tuning	Least Functionality	CM-7	Restrict NFS client requests to privileged ports
Services	Least Functionality	CM-7	Disable boot services
Services	Least Functionality	CM-7	Disable email server, (if system does not function as email server)
Services	Least Functionality	CM-7	Disable inetd
Services	Least Functionality	CM-7	Disable login prompts on serial ports
Services	Least Functionality	CM-7	Disable unused boot services
Services	Least Functionality	CM-7	Disable automount daemon
Services	Least Functionality	CM-7	Disable FTP
Services	Least Functionality	CM-7	Disable GSS daemon
Services	Least Functionality	CM-7	Disable Kerberos-related daemons
Services	Least Functionality	CM-7	Disable NFS server processes
Services	Least Functionality	CM-7	Disable printer service
Services	Least Functionality	CM-7	Disable removable media daemon
Services	Least Functionality	CM-7	Disable rlogin/rsh/rcp
Services	Least Functionality	CM-7	Disable rquotad
Services	Least Functionality	CM-7	Disable SNMP
Services	Least Functionality	CM-7	Disable SUN Volume Manager daemons
Services	Least Functionality	CM-7	Disable telnet
Services	Least Functionality	CM-7	Disable TFTP
Services	Least Functionality	CM-7	Disable the LDAP cache manager
Services	Least Functionality	CM-7	Disable the printer daemons
Services	Least Functionality	CM-7	Disable the volume manager

Category	800-53	Map	Action
Services	Least Functionality	CM-7	Disable Windows-compatibility
Services	Least Functionality	CM-7	Disable other RPC-based services
Accounts / Access	Authenticator Management	IA-5	No “+" entries should exist in /etc/passwd or /etc/group.

Table F-7. HP-UX Configuration Guide

Category	800-53	Map	Action
Accounts / Access	Account Management	AC-2	Configure the system per 800-53 Account Policy Control Requirements.
Accounts / Access	Account Management	AC-2	Lock system accounts to prevent them from being used to log in to the system
Accounts / Access	Account Management	AC-2	No '.' (current working directory) or group/world writable files exist in root's $PATH.
Accounts / Access	Account Management	AC-2	Remove user .netrc files
Accounts / Access	Account Management	AC-2	Install TCP Wrappers
Accounts / Access	Account Management	AC-2	Set "mesg n" as default for all users
Accounts / Access	Account Management	AC-2	Set default group for root account
Accounts / Access	Access Enforcement	AC-3	Create the /etc/[ftpd]/ftpusers file.
Accounts / Access	Access Enforcement	AC-3	Cron and At use is restricted to authorized users.
Accounts / Access	Access Enforcement	AC-3	Root logins are restricted to the system console only.
Accounts / Access	Access Enforcement	AC-3	The root account is the only account with UID 0.
Accounts / Access	Access Enforcement	AC-3	Set default UMASK for users, directories, and files to meet the needs of the system
Accounts / Access	Information Flow Enforcement	AC-4	Install TCP Wrappers to limit network access to the system.
Accounts / Access	System Use Notification	AC-8	Create warnings for GUI-based logins, FTP logins, and terminal-session logins
Accounts / Access	Authenticator Management	IA-5	No “+" entries should exist in /etc/passwd or /etc/group.
Auditing	Auditable Events	AU-2	Configure the system per 800-53 Audit Control Requirements.
Auditing	Protection of Audit Information	AU-9	Unless the host is functioning as a syslog server, prevent the system from accepting syslog messages from the network.
Installation / Patches	Transmission Integrity	SC-8	Utilize Secure Shell (SSH) for remote logins and file transfers.
Patches	Flaw Remediation	SI-2	Apply critical Operating System

Category	800-53	Map	Action
			security patches
Patches	Flaw Remediation	SI-2	Ensure That Before the System is Loaded Onto an Operational Network, Security Patches, Service Packs, And Hot Fixes are all Tested
Misc / Tuning	Information Flow Enforcement	AC-4	Kernel Tuning - Enable stack protection
Misc / Tuning	Information Flow Enforcement	AC-4	Kernel Tuning - Restrict core dumps to protected directory
Misc / Tuning	Information Flow Enforcement	AC-4	Kernel Tuning - Use better TCP sequence numbers
Misc / Tuning	Least Functionality	CM-7	Configure the system per 800-53 File Permissions/Access Control Requirements.
Misc / Tuning	Least Functionality	CM-7	Kernel Tuning - Restrict NFS client requests to privileged ports
Services	Remote Access	AC-17	Disable r-commands (rlogin, rcp, remsh) unless necessary.
Services	Remote Access	AC-17	Disable the Trivial File Transfer Protocol (TFTP). TFTP is normally used to boot diskless workstations over the network.
Services	Least Functionality	AC-17	Minimize boot services such as: BIND inetd printer daemons GUI logins web servers RPC-based services
Services	Remote Access	AC-17	Prevent connections to serial ports.
Services	Least Functionality	CM-7	Disable the Simple Network Management Protocol (SNMP) if it is not used for remote monitoring and management of TCP/IP devices.
Services	Least Functionality	CM-7	Disable the xdmcp port.
Services	Least Functionality	CM-7	If the system has an e-mail server that must be used, ensure it does not give out information about itself.
Services	Least Functionality	CM-7	Minimize inetd network services.

Category	*800-53*	*Map*	*Action*
Services	*Least Functionality*	*CM-7*	*Remove .rhosts and .netrc files from the system.*
Services	*Least Functionality*	*CM-7*	*Unless the system is used as a NFS server, disable the Network File System (NFS) server and client daemons.*
Services	*Least Functionality*	*CM-7*	*Unless the system is used as a NIS Server, disable the Network Information Service (NIS) processes.*
Services	*Least Functionality*	*CM-7*	*Disable X-Windows*
Logon	*User Identification and Authentication*	*IA-2*	*Configure the system to use an HHS accepted warning banner.*

Table F-8. RedHat Linux Configuration Guide

Category	800-53	Map	Action
Accounts / Access	Account Management	AC-2	No '.' (current working directory) or group/world writable files exist in root's $PATH.
Accounts / Access	Account Management	AC-2	Install TCP Wrappers
Accounts / Access	Account Management	AC-2	Remove user .netrc files
Accounts / Access	Account Management	AC-2	Set "mesg n" as default for all users
Accounts / Access	Account Management	AC-2	Set default group for root account
Accounts / Access	Account Management	AC-2	Verify that no UID 0 accounts exist other than root
Accounts / Access	Access Enforcement	AC-3	Set user home directories to be as restrictive as possible
Accounts / Access	Access Enforcement	AC-3	Set Account Expiration Parameters On Active Accounts
Accounts / Access	Access Enforcement	AC-3	Require Authentication For Single-User Mode
Accounts / Access	Access Enforcement	AC-3	Remove rhosts support in pam
Accounts / Access	Access Enforcement	AC-3	Remove empty crontab files and restrict file permissions to authorized users
Accounts / Access	Access Enforcement	AC-3	Restrict at/cron to authorized users
Accounts / Access	Access Enforcement	AC-3	Restrict root logins to system console
Accounts / Access	Access Enforcement	AC-3	Set LILO/GRUB Password
Accounts / Access	System Use Notification	AC-8	Set a warning banner for console and GUI based logins.
Auditing	Auditable Events	AU-2	Configure the system per 800-53 Audit Control Requirements.
Auditing	Auditable Events	AU-2	Enable system accounting (Install the sysstat package if needed).
Installation / Patches	Transmission Integrity	SC-8	Utilize Secure Shell (SSH) for remote logins and file transfers.
Patches,	Flaw Remediation	SI-2	Apply critical Operating System security patches
Misc / Tuning	Information Flow Enforcement	AC-4	Deny all network access to the system via hosts.deny; Explicitly allow network connections,

Category	800-53	Map	Action
			either all services selected ones, from the local network and selected hosts via hosts.allow
Misc / Tuning	Information Flow Enforcement	AC-4	Add ' nosuid' and ' nodev' Option For Removable Media In /etc/fstab
Auditing	Protection of Audit Information	AU-9	Unless the host is functioning as a syslog server, prevent the system from accepting syslog messages from the network.
Misc / Tuning	Least Functionality	CM-7	Set default UMASK for users, directories, and files to meet the needs of the system
Misc / Tuning	Least Functionality	CM-7	Disable Core Dumps
Services	Least Functionality	CM-7	Disable xinetd if none of its services are used
Services	Least Functionality	CM-7	Disable Sendmail
Services	Least Functionality	CM-7	Disable GUI Logon
Services	Least Functionality	CM-7	Disable X-Windows
Services	Least Functionality	CM-7	Disable standard boot services that do not support the role of the system
Services	Least Functionality	CM-7	Turn off standard services except those needed for the system’s role.
Logon	User Identification and Authentication	IA-2	Configure the system to use an HHS accepted warning banner.
Accounts / Access	Authenticator Management	IA-5	No “+" entries should exist in /etc/passwd or /etc/group.

Table F-9. Oracle Configuration Guide

Category	*800-53*	*Map*	*Action*
Accounts	*Access Enforcement*	*AC-2*	*Depending on the Oracle version specific environment, on the default accounts, drop the user, lock the user account, or change the default password.*
Accounts	*Access Enforcement*	*AC-2*	*Ensure that the SYS and SYSTEM account passwords are changed to a secure password from the defaults of change_on_install and manager.*
Accounts	*Access Enforcement*	*AC-3*	*To reduce the risk of unauthorized access, do not hardcode usernames and passwords in application source code.*
Password Management	*Access Enforcement*	*AC-3*	*Do not store passwords in clear text in Oracle tables.*
Password Management	*Access Enforcement*	*AC-3*	*Passwords for batch processes must not be a command line parameter or an environment variable.*
Password Management	*Access Enforcement*	*AC-3*	*Whenever utilizing silent installs, i.e., Oracle Installer, ensure configuration files do not contain password values after the installation completes.*
Access Controls	*Access Enforcement*	*AC-3*	*Set all default account passwords to non-default strong passwords. When installed, some third party applications create well-known default accounts in an Oracle database. The default password for these accounts must be changed or the account must be locked.*
Access Controls	*Access Enforcement*	*AC-3*	*Ensure that file permissions are securely set.*
Access Controls	*Access Enforcement*	*AC-3*	*Ensure that users profile settings have appropriate values set for any particular database and application.*
Access Controls	*Access Enforcement*	*AC-3*	*Ensure that users have the minimum permissions, roles and privileges required.*
Access Controls	*Access Enforcement*	*AC-3*	*When dropping a user, ensure roles and privileges created by*

Category	800-53	Map	Action
			that user, if not required, are deleted.
Access Controls	*Access Enforcement*	*AC-3*	*Revoke PUBLIC execute privileges for DBMS_JOB, DBMS_LOB, DBMS_SYS_SQL and DBMS_RANDOM.*
Access Controls	*Access Enforcement*	*AC-3*	*Standard ports for listener.ora are well known and can be used by attackers to verify applications running on a server.*
Access Controls	*Access Enforcement*	*AC-3*	*Ensure that a listener password is set.*
Audit	*Auditable Events*	*AU-2*	*Audit the following to ensure access is appropriate.* *Log-ons and log-offs.* *Any ALTER statement.* *Any CREATE statement.* *Any DROP statement.* *Any GRANT statement.* *Any unsuccessful attempts. (ACCESS WHENEVER NOT SUCCESSFUL)* *Any INSERT failures.*
Audit	*Auditable Events*	*AU-2*	*Use fine grain access control and auditing*
Access Controls	*Configuration Settings*	*CM-6*	*Purge policy caches.*
Access Controls	*Configuration Settings*	*CM-6*	*If extproc functionality is not required remove binary from host ($ORACLE_HOME/bin/extproc) and remove entry in tnsnames.ora.*
Logon	*User Identification and Authentication*	*IA-2*	*Configure the system to use an HHS accepted warning banner.*
Access Controls	*Access Enforcement*	*SC-4*	*Ensure that all critical data is encrypted .*
Network Access	*Transmission Confidentiality*	*SC-4*	*Ensure that any data sent over a network is secure or sent via a secure protocol.*
Patches	*Flaw Remediation*	*SI-2*	*Ensure that quarterly critical Patch Updates and any applicable Security Alerts are reviewed and applied in a timely manner.*

Table F-10. Cisco IOS Configuration Guide

Category	*800-53*	*Map*	*Action*
Access Controls	*Access Enforcement*	*AC-3*	*Don't use default SNMP community strings*
Access Controls	*Access Enforcement*	*AC-3*	*Define ACLs to allow only authorized connections to the router*
Access Controls	*Denial of Service Protection*	*SC-5*	*Explicitly disallow IP directed broadcast on each interface.*
Access Controls	*Denial of Service Protection*	*SC-5*	*Use tcp keepalives to kill sessions where the remote side has died. Stale connections use resources and could potentially be hijacked to gain illegitimate access.*
Access Controls	*Information Flow Enforcement*	*AC-4*	*Create Access Control Lists (ACLs) for all VTY lines*
Access Controls	*Least Functionality*	*CM-7*	*Disable SNMP if not in use*
Access Controls	*Least Functionality*	*CM-7*	*Bind AAA services to the loopback interface*
Access Controls	*Remote Access*	*AC-17*	*Permit only SSH for incoming VTY login (if available)*
Audit	*Auditable Events* *Audit Retention* *Protection of Audit Information*	*AU-2* *AU-5* *AU-11*	*Configure the system per 800-53 Audit Control Requirements.*
Audit	*Least Functionality*	*CM-7*	*Define and configure at least one loopback interface*
Audit	*Time Stamps*	*AU-8*	*Adjust to summertime if local time zone is used*
Audit	*Time Stamps*	*AU-8*	*Configure debug messages to include timestamps*
Audit	*Time Stamps*	*AU-8*	*Set time zone explicitly*
Passwords	*Access Enforcement*	*AC-3*	*Use AAA authentication methods*
Passwords	*Authenticator Management*	*IA-5*	*Encrypt passwords in configs*
Passwords	*Authenticator Management*	*IA-5*	*Set an enable secret*
Passwords	*Authenticator Management*	*IA-5*	*Configure the system per 800-53 Account Policy Control Requirements.*
Services	*Least Functionality*	*CM-7*	*Review servers for necessity, and disable if not needed. (ex. bootp,*

Category	800-53	Map	Action
			http, finger, identd, tftp, etc)
Services	Least Functionality	CM-7	Disable Cisco Discovery Protocol (CDP) service
Services	Least Functionality	CM-7	Disable Configuration Auto-Loading
Services	Least Functionality	CM-7	Disable exec on aux
Services	Least Functionality	CM-7	Disable proxy ARP on all interfaces
Services	Least Functionality	CM-7	Disable source routing
Services	Least Functionality	CM-7	Disable unnecessary services such as echo, discard, chargen, etc.
Sessions	Session Lock	AC-11	Disconnect sessions after a fixed idle time
Time	Time Stamps	AU-8	Designate a second NTP time server
Time	Time Stamps	AU-8	Designate an NTP time server
User Accounts	Account Management	AC-2	Automatically terminating/disabling temporary accounts after a set period of time.
User Accounts	User Identification and Authentication	IA-2	Create Emergency Local User Account

Appendix G:
Acronyms and Abbreviations

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

A

AAL	Authorized Access List
ABMAC	*A/B Medicare Administrative Contractor*
AC	Alternating Current
ADM	Administrative
ADP	Automated Data Processing
AFE	Annual Frequency Estimate
AIE	Annual Impact Estimate
AIS	Automated Information System
AISSP	Automated Information Systems Security Program
ALE	Annual Loss Expectancy
ANSI	American National Standards Institute
APF	Authorized Program Facility
ARO	Annualized Rate of Occurrence
ASC	Accredited Standards Committee

B

BI	Background Investigation
BIA	Business Impact Analysis

C

C&A	Certification and Accreditation
CAP	Corrective Action Plan
CAST	Contractor Assessment Security Tool
CCMO	Consortium Contractor Management Officer
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CICG	Critical Infrastructure Coordination Group
CIO	Chief Information Officer
CIS	Center for Internet Security
CISS	CMS Integrated Security Suite
CMP	Configuration Management Plan
CO	Central Office
COMSEC	Communication Security

CMS	Centers for Medicare and Medicaid Services
CPIC	Certification Package for Internal Controls
CPU	Central Processing Unit
CSAT	Computer Security Awareness Training
CSIRC	Computer Security Incident Response Capability
CSR	Core Security Requirement
CWF	Common Working File

D

DASD	Direct Access Storage Devices
DBA	Database Administrators
DBM	Database Management
DC	District of Columbia
DBMS	Database Management System
DES	Data Encryption Standard
DHHS	Department of Health and Human Services
DISA	Defense Investigative Security Agency
DME*MAC*	Durable Medical Equipment *Medicare Administrative Contractor*
DOS	Denial of Service
DSL	Digital Subscriber Line
DSS	Digital Signature Standard

E

EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EF	Exposure Factor
E-mail	Electronic Mail
EO	Executive Orders
EVA	External Vulnerability Assessment

F

FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FTI	Federal Tax Information (or Federal tax return information)

G

GAO	General Accounting Office
GSA	General Services Administration
GSS	General Support System

H

HIPAA	Health Insurance Portability and Accountability Act
HISM	Handbook of Information Security Management
HITR	HCFA Information Technology Reference
HSPD	Homeland Security Presidential Directive

I

IA	Information Assurance
IBM	International Business Machines (Corp.)
ID	Identification
IDS	Intrusion Detection System
INFOSEC	Information Systems Security
IP	Internet Protocol
IPL	Initial Program Load
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IRSAP	Internal Revenue Service Acquisition Procedure
ISSO	Information Systems Security Officer
IT	Information Technology
ITMRA	Information Technology Management Reform Act

L

LAN	Local Area Network

M

MA	Major Application
MAC	Medicare Administrative Contractor
MBI	Minimum Background Investigation
MBSA	Microsoft Baseline Security Analyzer
MCM	Medicare Carriers Manual
MCS	Multiple Console Support
MDCN	Medicare Data Communications Network
MIM	Medicare Intermediary Manual
MISPC	Minimum Interoperability Specification for PKI Components
MMA	Medicare Prescription Drug, Improvement, and Modernization Act of 2003
MPS	Minimum Protection Standard
MVS	Multiple Virtual Storage

N

NARA	National Archives and Records Administration
NC	Network Computer

NCSC	National Computer Security Center
NIE	Net Impact Estimate
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NOS	Network Operating System
NSA	National Security Agency
NSC	National Security Council
NSTISSI	National Security Telecommunications and Information Systems Security Committee
NT	New Technology

O

OIG	Office of Inspector General
OIS	Office of Information Services (CMS)
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OTC	On-Time-Cost

P

PC	Personal Computer
PDA	Personal Digital Assistants
PDD	Presidential Decision Directive
PDS	Partitioned Data Sets
PIN	Personal Identification Number
PISP	*Policy for the Information Security Program*
PKI	Public Key Infrastructure
PM	Project (Program) Managers
PO	Project Officer
POA&M	Plan of Action and Milestones
PSGH	CMS Policy Standards and Guidelines Handbook
PSO	Physical Security Officer
PUB	Publication

R

RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFP	Requests for Proposals
RO	Regional Office
ROM	Read Only Memory

S

SA	Security Administrator
SAR	Safeguard Activity Report
SBI	Single Scope Background Investigation (SBI)
SBU	Sensitive but unclassified
SDLC	System Development Life Cycle
SER	Scientific, Engineering, and Research
SHS	Secure Hash Standard
SII	Security/Suitability Investigation Index
SIRT	Security Incident Response Team
SLE	Single Loss Expectancy
SM	System Manager
SMF	System Management Facility
S-MIME	Secure Multi-purpose Internet Mail Extensions
SOW	Statement of Work
SPR	Safeguard Procedures Report
SSA	Social Security Administration
SSC	Systems Security Coordinator
SSL	Secure Socket Layer
SSM	Shared System Maintainers
SSO	Systems Security Officer
SSP	System Security Plan
SSPM	System Security Plans Methodology
SSSA	Senior Systems Security Advisor
STIG	Security Technical Implementation Guide

T

TCP	Transmission Control Protocol
TDES	Triple Data Encryption Algorithm
TLS	Transport Layer Security
TO	Training Office

U

UID	User Identification
UL	Underwriter's Laboratory
U.S.C	United States Code

V

VoIP	Voice over IP

W

WAN	Wide Area Network

Appendix H:
Glossary

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Term	Definition
Access	(1) A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (NCSC-TG-004) (2) Opportunity to make use of an information system resource. (CNSS)
Access Control	Controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access controls include both physical access controls, which limit access to facilities and associated hardware, and logical controls, which prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically. (FISCAM)
Access Control Facility	An access control software package marketed by Computer Associates International, Inc. (FISCAM)
Access Control Software	This type of software (CA-ACF2, RACF, CA-TOP SECRET), which is external to the operating system, provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a wanting, or allowing access to all resources without warning regardless of authority. (FISCAM)
Access Method	The technique used for selecting records in a file for processing, retrieval, or storage. (FISCAM)
Access Path	(1) The path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc. (FISCAM) (2) Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path.
Access Privileges	Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on the system, and under what circumstances this access will be allowed. (FISCAM)

Accountability	The existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established. (FISCAM)
Accreditation	(1) The official management authorization for the operation on an application and is based on the certification process as well as other management considerations. (Automated Information Systems Security Program Handbook [AISSP]) (FIPS PUB 102) (2) A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (NCSC-TG-004)
Action Plan	Part of the CISS functionality, an action plan is a record that indicates the methods by which one or more weaknesses are to be mitigated. An action plan contains milestones and projected completion dates, and is included in the POA&M submission package and any POA&M reports. An action plan is not to be confused with the quarterly CAP submission that Business Partners make to CMS, because the scope of the CAP submission (which contains financial data) exceeds the scope of the CISS.
Application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. (FISCAM)
Application Controls	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. (FISCAM)
Application Programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities. (FISCAM)
Application Programs	See Application.
Application System(s)	A computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system. (AISSP) (FIPS PUB 11-3)
Application System Manager	See Application Manager.

Asset	Any software, data, hardware, administrative, physical communications, or personnel resource within an ADP system of activity.
Attack	The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (NCSC-TG-004)
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (CNSS)
Audit Software	Generic audit software consists of a special program or set of programs designed to audit data stored on computer media. Audit software performs functions such as data extraction and reformatting, file creation, sorting, and downloading. This type of audit software may also be used to perform computations, data analysis, sample selection, summarization, file stratification, field comparison, file matching, or statistical analysis. The term audit software may also refer to programs that audit specific functions, features, and controls associated with specific types of computer systems to evaluate integrity and identify security exposures. (FISCAM)
Audit Trail	In an accounting package, any program feature that automatically keeps a record of transactions so you can backtrack to find the origin of specific figures that appear on reports. In computer systems, a step-by-step history of a transaction, especially a transaction with security sensitivity. Includes source documents, electronic logs, and records of accesses to restricted files. (FISCAM)
Authentication	The act of verifying the identity of a user and the user's eligibility to access computerized information. Designed to protect against fraudulent activity. (FISCAM)
Automated Information System (AIS)	The organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. (AISSP) (OMB Circular A-130)
Automated Information Systems Security	See Systems Security.
Backup	Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource. (FISCAM)
Backup Plan	See Contingency Plans.

Backup Procedures	A regular maintenance procedure that copies all new or altered files to a backup storage medium, such as a tape drive. (FISCAM)
Batch (Processing)	A mode of operation in which transactions are accumulated over a period of time, such as a day, week, or month, and then processed in a single run. In batch processing, users do not interact with the system while their programs and data are processing as they do during interactive processing. (FISCAM)
Biometric Authentication	The process of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometric devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. (FISCAM)
Breach(es)	The successful and repeatable defeat of security controls with or without an arrest, which if carried to consummation, could result in a penetration of the system. Examples of breaches are: • Operation of user code in master mode. • Unauthorized acquisition of identification password or file access passwords. • Accessing a file without using prescribed operating system mechanisms. • Unauthorized access to tape library.
Browsing	(1) The act of electronically perusing files and records without authorization. (FISCAM) (2) The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (NCSC-TG-004)
Business Partners	Non-federal personnel who perform services for the federal government at a site owned by the partner under the terms and conditions of a contractual agreement. Business Partners need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements. *Business Partners include Medicare carriers, Fiscal Intermediaries, Common Working File host sites, standard claims processing system maintainers, regional laboratory carriers, claims processing data centers, Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors (DMEMAC), A/B Medicare Administrative Contractors (ABMAC) and Enterprise Data Centers (EDCs).*

Certification (Recertification)	(1) Consists of a technical evaluation of a sensitive application to see how well it meets security requirements. (AISSP) (FIPS PUB 102) (2) A formal process by which an agency official verifies, initially or by periodic reassessment, that a system's security features meet a set of specified requirements.
Checkpoint	The process of saving the current state of a program and its data, including intermediate results to disk or other nonvolatile storage, so that if interrupted the program could be restarted at the point at which the last checkpoint occurred. (FISCAM)
Chief Information Officer (CIO)	The CIO is responsible for the implementation and administration of the AIS Security Program within an organization.
Cipher Key Lock	A lock with a key pad-like device that requires the manual entry of a predetermined code for entry. (FISCAM)
Classified Resources/ Data/Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (CNSS)
Code	Instructions written in a computer programming language. (See object code and source code.) (FISCAM)
Cold Site	An information system backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative computing location. (FISCAM)
Command(s)	A job control statement or a message, sent to the computer system, that initiates a processing task. (FISCAM)
Communications Program	A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks. (FISCAM)
Communications Security (COMSEC)	Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto-security, transmission security, emission security, and physical security of COMSEC material. (CNSS)
Compact Disc-Read Only Memory (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally read-only. (FISCAM)

Compatibility	The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are key to achieving compatibility. (FISCAM)
Compensating Control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions. (FISCAM)
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components. (FISCAM)
Compromise	An unauthorized disclosure or loss of sensitive defense data. (FIPS PUB 39)
Computer	See Computer System.
Computer Facility	A site or location with computer hardware where information processing is performed or where data from such sites is stored. (FISCAM)
Computer Network	See Network.
Computer Operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems. (FISCAM)
Computer-related Controls	Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications. (FISCAM)
Computer Resource	See Resource.
Computer Room	Room within a facility that houses computers and/or telecommunication devices. (FISCAM)
Computer Security	See Information Systems Security and Systems Security.
Computer Security Incident Response Capability (CSIRC)	That part of the computer security effort that provides the capability to respond to computer security threats rapidly and effectively. [A CSIRC provides a way for users to report incidents, and it provides personnel and tools for Investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents.] (AISSP – Source: NIST SP 800-3)

Computer System	(1) A complete computer installation, including peripherals, in which all the components are designed to work with each other. (FISCAM) (2) Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (AISSP) (Computer Security Act of 1987)
Confidentiality	Ensuring that transmitted or stored data is not read by unauthorized persons. (FISCAM)
Configuration Management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. (FISCAM)
Compliance	Refers to the current set of reporting obligations arising from the contractual obligations of business partners to CMS.
Console	Traditionally, a control unit such as a terminal through which a user Communicates with a computer. In the mainframe environment, a Console is the operator's station. (FISCAM)
Consortium	Currently consists of four CMS offices (Northeastern, Southern, Midwestern, and Western) that oversee the operations at the Regional Offices.
Consortium Contractor Management Officer (CCMO)	Part of the Regional Consortiums, the CCMO is responsible for leading and directing contractor management at the consortium level.
Contingency Plan(s)	(1) Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster. (FISCAM) (2) A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (AISSP) (FIPS PUB 11-3)
Contingency Planning	(1) The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. (ISSPH - Glossary) (2) See contingency plan. (FISCAM)

Contractors	Non-federal personnel who perform services for the federal government under the terms and conditions of a contractual agreement. Contractors need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.
Control Technique	Statements that provide a description of what physical, software, procedural or people related condition must be met or in existence in order to satisfy a core requirement. (Appendix A.)
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text or plain text and other data are transformed into coded form by encryption and translated back to plain text or data by decryption. (FISCAM)
Data	Facts and information that can be communicated and manipulated. (FISCAM)
Data Administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. (FISCAM)
Data Center	See Computer Facility.
Data Communications	(1) The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM) (2) The transfer of data between functional units by means of data transmission according to a protocol. (AISSP) (FIPS PUB 11-3)
Data Control	The function responsible for seeing that all data necessary for processing are present and that all output is complete and distributed properly. This function is generally responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing. (FISCAM)
Data Dictionary	A repository of information about data, such as their meanings, relationships to other data, origin, usage, and format. The dictionary assists company management, database administrators, systems analysts, and application programmers in effectively planning, controlling, and evaluating the collection, storage, and use of data. (FISCAM)

Data Encryption Standard (DES)	(1) A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data. (FISCAM) (2) The National Institute of Standards and Technology Data Encryption Standard was adopted by the U.S. Government as Federal Information Processing Standard (FIPS) Publication 46 [at publication 46-1], which allows only hardware implementations of the data encryption algorithm. (AISSP) (FIPS PUB 11-3)
Data File	See File.
Data Owner	See "Owner." (FISCAM)
Data Processing	The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing. (FISCAM)
Data Security	(1) The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (FIPS PUB 39) (2) See Security Management Function.
Data Validation	Checking transaction data for any errors or omissions that can be detected by examining the data. (FISCAM)
Database	(1) A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer. (FISCAM) (2) A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (AISSP) (FIPS PUB 11-3)
Database Administrator (DBA)	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database. (FISCAM)
Database Management (DBM)	Tasks related to creating, maintaining, organizing, and retrieving information from a database. (FISCAM)
Database Management System (DBMS)	A software product (DB2, IMS, IDMS) that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions, such as queries or updates from users, and permit centralized control of security and data integrity. (FISCAM)
DBMS	See Database Management System.

Debug (Software)	To detect, locate, and correct logical or syntactical errors in a computer program. (FISCAM)
Degauss	To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (FIPS PUB 39)
Denial of Service (DOS)	Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Synonymous with interdiction. (NCSC-TG-004)
DES	See Data Encryption Standard.
Dial-up(in) Access	A means of connecting to another computer or a network like the Internet, over a telecommunications line using a modem-equipped computer. (FISCAM)
Dial-up Security Software	Software that controls access via remote dial-up. One method of preventing unauthorized users from accessing the system through an unapproved telephone line is through dial-back procedures in which the dial-up security software disconnects a call initiated from outside the network via dial-up lines, looks up the user's telephone number, and uses that number to call the user. (FISCAM)
Disaster Plan	See Contingency Plan.
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (FISCAM)
Disclosure (Illegal Access and Disclosure)	Activities of employees that involve improper systems access and sometime disclosure of information found thereon, but not serious enough to warrant criminal prosecution. These cases should be entered on the Fraud Monitoring and Reporting System.
Disk Storage	High-density random access magnetic storage devices that store billions of bits of data on round, flat plates that are either metal or plastic. (FISCAM)
Diskette	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case. (FISCAM)
Electronic Data Interchange (EDI)	A standard for the electronic exchange of business documents, such as invoices and purchase orders. Electronic data interchange (EDI) eliminates intermediate steps in processes that rely on the transmission of paper-based instructions and documents by performing them electronically, computer to computer. (FISCAM)

Electronic Mail (e-mail)	The transmission of memos and messages over a network. Within an enterprise, users can send mail to a single recipient or broadcast it to multiple users. With multitasking workstations, mail can be delivered and announced while the user is working in an application. Otherwise, mail is sent to a simulated mailbox in the network server or host computer, which must be interrogated. An e-mail system requires a messaging system, which provides the store and forward capability, and a mail program that provides the user interface with send and receive functions. The Internet revolutionized e-mail by turning countless incompatible islands into one global system. The Internet initially served its own members, of course, but then began to act as a mail gateway between the major online services. It then became "the" messaging system for the planet. (TechEncy)
Electronic Signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. (FISCAM)
Encryption	The transformation of data into a form readable only by using the appropriate key held only by authorized parties. (FISCAM)
End User(s)	Employees who have access to computer systems and networks that process, store, or transmit information. This is the largest and most heterogeneous group of employees. It consists of everyone, from an executive with a desktop system to application programmers to data entry clerks.
Environmental Controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls. (FISCAM)
Exception Criteria	Exception criteria refers to batch processes that return files or records as not meeting certain predefined criteria for processing.
Execute (Access)	This level of access provides the ability to execute a program. (FISCAM)
Facility(ies)	See Computer Facility.
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record. (FISCAM)
File	A collection of records stored in computerized form. (FISCAM)

Firewall	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. (FISCAM)
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. (FISCAM)
General Controls	The structure, policies, and procedures that apply to an entity's overall computer operations. These include an entity-wide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls. (FISCAM)
General Support System(s) (GSS)	(1) An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a general support system is to provide processing or communication support. (FISCAM) (2) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (OMB Circular A-130)
Guided Media	(1) Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable) (2) Provides a closed path between sender and receiver • Twisted Pair (e.g. Telephone cable) • Coaxial Cable • Optical Fiber (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
Handled	(As in "Data handled.") Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.

Hardware	The physical components of IT, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. (FISCAM)
Hot Site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster. (FISCAM)
Image	An exact copy of what is on the storage medium
Implementation	The process of making a system operational in the organization. (FISCAM)
Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.
Information	(1) The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people. (FISCAM) (2) Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (AISSP) (OMB Circular A-130)
Information Resource	See Resource.
Information Resource Owner	See Owner.
Information System	The entire collection of infrastructure, organization, personnel, and components used to collect, process, store, transmit, display, disseminate, and dispose of information.
Information Systems Security (INFOSEC)	The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including cryptosecurity, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (AISSP) (NISTIR 4659)
Information Systems Security Officer (ISSO)	(1) Individual responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.
Information Technology (IT)	(1) Processing information by computer. (TechEncy) (2) IT or Information Technology has probably been the most redefined term over the past few years. The definition has varied from simple automation of manual processes using micro-processors to computers to networks to desktop publishing to networking. (Source: U. Texas)

Initial Program Load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program. (FISCAM)
Input	Any information entered into a computer or the process of entering data into the computer. (FISCAM)
Integrity	With respect to data, their accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users. (FISCAM)
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user. (FISCAM)
Internal Control	A process, effected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring. (Also referred to as Internal Control Structure) (FISCAM)
Internet	When capitalized, the term "Internet" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
Investigation(s)	The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system.
IPL	See Initial Program Load.
Job	A set of data that completely defines a unit of work for a computer. A job usually includes programs, linkages, files, and instructions to the operating system. (FISCAM)
Junk Mail (e-mail)	Transmitting e-mail to unsolicited recipients. U.S. federal law 47USC227 prohibits broadcasting junk faxes and e-mail, allowing recipients to sue the sender in Small Claims Court for $500 per copy. (TechEncy)
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message. (FISCAM)

Key Management	Supervision and control of the process whereby a key is generated, stored, protected, transferred, loaded, used, and destroyed.
Keystroke Monitoring	A process whereby computer system administrators view or record both the keystrokes entered by a computer user and the computer's response during a user-to-computer session. (AISSP – Source: CSL Bulletin)
Library	In computer terms, a library is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a library, each program is called a member. Libraries are also called partitioned data sets (PDS). Library can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries. (FISCAM)
Library Control/ Management	The function responsible for controlling program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. (FISCAM)
Library Management Software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes. (FISCAM)
Life-Cycle Process Life-Cycle Model	(1) Spans the entire time that a project/program including hardware and software is being planned, designed, developed, procured, installed, used, and retired from service. (2) A framework containing the processes, activities and tasks involved in the development, operation and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use. (Source: ISO/IEC 12207)
Limited Background Investigation (LBI)	This investigation consists of a NACI, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years. (SSPS&GH - Glossary)
Load Library	A partitioned data set used for storing load modules for later retrieval. (FISCAM)
Load Module	The results of the link edit process. An executable unit of code loaded into memory by the loader. (FISCAM)

Local Area Network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. Local area networks commonly include microcomputers and shared (often-expensive) resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks. (FISCAM)
Log(s)	With respect to computer systems, to record an event or transaction. (FISCAM)
Log Off	The process of terminating a connection with a computer system or peripheral device in an orderly way. (FISCAM)
Log On (Log In)	The process of establishing a connection with, or gaining access to, a computer system or peripheral device. (FISCAM)
Logging File	See Log(s) above.
Logic Bomb	In programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. (FISCAM)
Logical Access Control	The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges. (FISCAM)
Mail Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system. (TechEncy)
Mainframe System (Computer)	A multi-user computer designed to meet the computing needs of a large organization. The term came to be used generally to refer to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations. (FISCAM)
Maintenance	(1) Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time. (FISCAM) (2) The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions. (Source: IEEE Std 610.12-1990)
Major Application (MA)	(1) OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application. (FISCAM) (2) An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss,

	misuse, modification of, or unauthorized access to the information in the application. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A major application can be either a major software application or a combination of hardware/software. Its sole purpose is to support a specific mission-related function. (ISSPH - Glossary) (3) An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB Circular A-130) All "Major Applications" require "special management attention." The System Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.
Malicious Software (Code)	The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (AISSP – Source: DHHS Definition, adapted from NIST SP 500-166)
Management Controls	The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used consistent with the organization's mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision-making. (FISCAM)
Master Console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands. (FISCAM)
Master File(s)	In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period. (FISCAM)
Material	Refers to data processed, stored, or used in and information generated by an ADP system regardless of form or medium (e.g., programs, reports, data sets or files, records, and data elements).

Media	The physical object such as paper, PC, and workstation diskettes, CD-ROMs, and other forms by which CMS data are stored or transported. The risk to exposure is considered greater when data are in an electronically readable and transmittable form than when the same data are in paper-only form. This is due to the greater volume of information that can be sent in electronic form, the ease and convenience with which the information can be transmitted, and the potential that such information will be intercepted or inadvertently sent to the wrong person or entity.
Methodology	The specific way of performing an operation that implies precise deliverables at the end of each stage. (TechEncy)
Migration	A change from an older hardware platform, operating system, or software version to a newer one. (FISCAM)
Minimum Background Investigation (MBI)	This investigation includes a NACI, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. The MBI is an enhanced version of the NACIC and can be used for selected public trust positions.
Mission Critical	Vital to the operation of an organization. In the past, mission critical information systems were implemented on mainframes and minicomputers. Increasingly, they are being designed for and installed on personal computer networks. (TechEncy)
Misuse of Government Property	The use of computer systems for other than official business that does not involve a criminal violation but is not permissible under CMS policies.
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received. (FISCAM)
Modification	Loss of integrity of an asset or asset group through the intentional or unintentional alteration of the asset or asset group.
National Agency Check (NAC)	An integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary.
Need-To-Know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. (CNSS)

Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. (FISCAM)
Non-privileged Access	Cannot bypass any security controls.
Object Code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program. (FISCAM)
Office of Information Services (OIS)	CMS Office that ensures the effective management of CMS's information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.
On-line	Available for immediate use. It typically refers to being connected to the Internet or other remote service. When you connect via modem, you are online after you dial in and log on to your Internet provider with your username and password. When you log off, you are offline. With cable modem and DSL service, you are online all the time. A peripheral device (terminal, printer, etc.) that is turned on and connected to the computer is also online. (TechEncy)
Operating System(s) (OS)	The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running. (FISCAM)
Operational Controls	These controls relate to managing the entity's business and include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards, and (3) does what management directs it to do. (FISCAM)
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy. (FISCAM)
Output Devices	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system. (FISCAM)
Owner	Manager or director with responsibility for a computer resource, such as a data file or application program. (FISCAM)
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs. (FISCAM)

Passwords	(1) A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) (2) Most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications is often easy to circumvent if the user has access to the operating system (and knowledge of what to do).
PDS	See Partitioned Data Set.
Penetration	Unauthorized act of bypassing the security mechanisms of a system. (CNSS)
Penetration Test	An activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.
Peripheral	A hardware unit that is connected to and controlled by a computer, but external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer. (FISCAM)
Personnel Controls	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause. (FISCAM)
Personal Data	Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
Personnel Security	Refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access. (AISSP – Source: NISTIR 4659) (Also see Personnel Controls)
Physical Access Control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment. (FISCAM)

Physical Security	Refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (SSPS&GH - Glossary) (Source: NISTIR 4659) (Also see Physical Access Control)
Port	An interface between the CPU of the computer and a peripheral device that governs and synchronizes the flow of data between the CPU and the external device. (FISCAM)
Privacy Information	The individual's right to privacy must be protected in Federal Government information activities involving personal information. Such information is to be collected, maintained, and protected so as to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. (OMB Circular A-130)
Privileged Access	Can bypass, modify, or disable the technical or operational system security controls.
Privileges	Set of access rights permitted by the access control system. (FISCAM)
Probe	Attempt to gather information about an information system or its users.
Processing	The execution of program instructions by the computer's central processing unit. (FISCAM)
Production Control	The function responsible for monitoring the information into, through, and scheduling and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task. (FISCAM)
Production Environment	The system environment where the agency performs its operational information processing activities. (FISCAM)
Production Programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management. (FISCAM)
Profile	A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. (See Standard Profile and User Profile.) (FISCAM)

Program	(1) A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system program, source programs, and object programs are all software programs. (FISCAM) (2) Consists of organized activity that contains ay number of basic elements such as conducting risk assessments; conducting IT security training; establishing an incident response capability; writing, establishing, and enforcing policies and procedures, and processes for planning, implementing, evaluating, and implementing remedial action for addressing weaknesses. (Title III of the E-Government Act)
Program Library	See Library.
Programmer	A person who designs, codes, tests, debugs, and documents computer programs. (FISCAM)
Programming Library Software	A system that allows control and maintenance of programs for tracking purposes. The systems usually provide security, check out controls for programs, and on-line directories for information on the programs. (FISCAM)
Project Officer (PO)	CMS official (generally located in Central Office business components) responsible for the oversight of other Business Partners. These include Common Working File (CWF) Host Sites, Durable Medical Equipment *Medicare Administrative Contractor* (DME*MAC*), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased. (FISCAM)
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data. (FISCAM)
Public Access Controls	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records. (FISCAM)
Public Domain Software	Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances. (FISCAM)
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (CNSS)

Public Trust Positions	Positions that have the potential for action or inaction by their incumbents to affect the integrity, efficiency, or effectiveness of assigned Government activities. The potential for adverse effects includes action or inaction that could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. (Source: 5 CFR Part 731)
Quality Assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures, and (2) the software meets the functional specifications defined by the user. (FISCAM)
Read Access	This level of access provides the ability to look at and copy data or a software program. (FISCAM)
Real-time System	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed. (FISCAM)
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item. (FISCAM)
Recovery Procedures	Actions necessary to restore data files of an information system and computational capability after a system failure. (CNSS)
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior. (FISCAM)
Remote Access	The process of communicating with a computer located in another place over a communications link. (FISCAM)
Resource(s)	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and non-computerized records. (FISCAM)
Resource Access Control Facility (RACF)	An access control software package developed by IBM. (FISCAM)
Resource Owner	See Owner. (FISCAM)
Review and Approval	The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network.

Risk	The potential for harm or loss is best expressed as the answers to these four questions: • What could happen? (What is the threat?) • How bad could it be? (What is the impact or consequence?) • How often might it happen? (What is the frequency?) • How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" per se. (HISM)
Risk Analysis	(1) The identification and study of the vulnerability of a system and the possible threats to its security. (AISSP – Source: FIPS PUB 11-3) (2) This term represents the process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures. (HISM)
Risk Assessment	(1) The identification and analysis of possible risks in meeting the agency's objectives that forms a basis for managing the risks identified and implementing deterrents. (FISCAM) (2) This term represents the assignment of value to assets, threat frequency (annualized), consequence (i.e., exposure factors), and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied. The term risk assessment is used to characterize both the process and the result of analyzing and assessing risk. (HISM)
Risk Evaluation	This task includes the evaluation of all collected information regarding threats, vulnerabilities, assets, and asset values in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur. Results are usually expressed in monetary terms on an annualized basis (ALE) or graphically as a probabilistic "risk curve" for a quantitative risk assessment. For a qualitative risk assessment, results are usually expressed through a matrix of qualitative metrics such as ordinal ranking (low, medium, high, or 1, 2, 3). (HISM)

Risk Management	(1) A management approach designed to reduce risks inherent to system development and operations. (FISCAM) (2) The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (AISSP – Source: NISTIR 4659) (3) This term characterizes the overall process. The first, or risk assessment, phase includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk. The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process of ever-increasing complexity. (HISM)
Resource	Any agency Automated Information System (AIS) asset. (AISSP – Source: DHHS Definition)
Router	An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route. (FISCAM)
Rules of Behavior	Rules for individual users of each general support system or application. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training. (OMB Circular A-130)
Run	A popular, idiomatic expression for program execution. (FISCAM)
Run Manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. (FISCAM)
Safeguard	This term denotes existing or required controls necessary to mitigate risk for a known weakness or vulnerability.
Sanction	Sanction policies and procedures are actions taken against employees who are non-compliant with security policy.
SDLC methodology	See System Development Life Cycle Methodology.
Section 912	Refers to the “Medicare Prescription Drug, Improvement, and Modernization Act of 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors.”

Security	(1) The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability. (FISCAM) (2) A technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishments. Also referred to as IT security. (NIST SP 800-16)
Security Administrator (SA)	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks. (FISCAM)
Security Awareness	(1) Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. (NIST SP 800-16) (2) Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences. (NIST SP 800-50)
Security Certification	A formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications. To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system. (NIST Special Publication 800-12)
Security Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.
Security Level Designation	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse) and the operational criticality of data processing capabilities (i.e., the consequences were data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an AIS is assigned for the overall security level designation. (AISSP – Source: DHHS Definition)

Security Management Function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness. (FISCAM)
Security Plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. (FISCAM)
Security Policy	The set of laws, rules, and practices that regulate how an Organization manages, protects, and distributes sensitive information. (NCSC-TG-004)
Security Profile	See Profile.
Security Program	(1) An entity-wide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. (FISCAM) (2) A program established, implemented, and maintained to ensure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its IT systems. (NIST SP 800-16)
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (CNSS)
Security Requirements Baseline	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security. (CNSS)
Security Software	See Access Control Software.
Security Training	(1) Security training teaches people the [security] skills that will enable them to perform their jobs more effectively. (NIST SP 800-16) (2) Training strives to produce relevant and needed security skills and competencies. (NIST SP 800-50)
Sensitive Application	An application of IT that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (AISSP – Source: OMB Circular A-130)
Sensitive Data	(1) Data that require protection due to the risk and magnitude of

	loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (AISSP – Source: OMB Circular A-130) (2) Information whose loss, misuse, unauthorized access to, modification, or destruction, could adversely affect the national interest or the conduct of Federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. (FIPS Pub 102)
Sensitive Information	(1) Any information whose loss, misuse, unauthorized access, unauthorized disclosure, or improper modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. (from FISCAM) (2) Any information whose loss, misuse, unauthorized access, unauthorized disclosure, or improper modification could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (from the AISSP – Source: Computer Security Act of 1987) (3) CMS Sensitive Information corresponds to "Level-3, High Sensitivity," described in section 4.1.1.3 of this document.
Sensitivity	The degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components. (NIST SP 800-16)
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network. (FISCAM)
Service continuity controls	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (FISCAM)

Significant Change	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (AISSP – Source: DHHS Definition)
Single Loss Expectancy (SLE)	This value is classically derived from the following algorithm to determine the monetary loss (impact) for each occurrence of a threatened event: ASSET VALUE X EXPOSURE FACTOR = SLE The SLE is usually an end result of a business impact analysis (BIA). A BIA typically stops short of evaluating the related threats' ARO or its significance. The SLE represents only one element of risk, the expected impact, monetary or otherwise, of a specific threat event. Because the BIA usually characterizes the massive losses resulting from a catastrophic event, however improbable, it is often employed as a scare tactic to get management attention and loosen budgetary constraints, often unreasonably. (HISM)
Smart Card	A credit card sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services. (FISCAM)
SMF	See System Management Facility.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text. (FISCAM)
Software	A computer program or programs, in contrast to the physical environment on which programs run (hardware). (FISCAM)
Software Life Cycle	The phases in the life of a software product, beginning with its conception and ending with its retirement. These stages generally include requirements analysis, design, construction, testing (validation), installation, operation, maintenance, and retirement. (FISCAM)
Software Security	General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system. (NCSC-TG-004)
Source Code	Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable. (FISCAM)
Special Management Attention	Some systems require "special management attention" to security due to the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access to, or modification of the information in the system. (OMB Circular A-130)

SSPS&G Handbook	Systems Security Policy Standards and Guidelines Handbook.
Stand-alone System (Computer)	A system that does not require support from other devices or systems. Links with other computers, if any, are incidental to the system's chief purpose. (FISCAM)
Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development. (FISCAM)
Standard Profile	A set of rules that describes the nature and extent of access to each resource that is available to a group of users with similar duties, such as accounts payable clerks. (FISCAM)
System	(1) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (OMB Circular A-130) (2) Refers to a set of information resources under the same management control that share common functionality and require the same level of security controls. The phase "General Support Systems (GSS)" as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications (MA)," as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, control software, or software for command and control). By categorizing both "General Support Systems" and "Major Applications" as "systems", unless explicitly stated, the procedures and guidance can address both in a simplified manner. When writing the required System Security Plans, two formats are provided--one for General Support Systems, and one for Major Applications. This ensures that the differences for each are addressed (CMS, System Security Plans (SSP) Methodology , July 2000, SSPM. A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system’s hardware may include mainframe systems, desktop systems (e.g., PC’s, Macintoshes, laptops, handheld devices), workstations and servers (e.g., Unix, NT, NC), local area networks (LAN), and any other platform regardless of the operating system.
System Administrator	The person responsible for administering use of a multi-user computer system, communications system, or both. (FISCAM)
System Analyst	A person who designs a system. (FISCAM)

System Development Life Cycle (SDLC) Methodology	The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle. (FISCAM)
System Life Cycle	(1) The period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The system life cycle is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase. (AISSP – Source: FIPS PUB 101) (Also see Software Life Cycle)
System Management Facility	An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage. (FISCAM)
System Manager (SM)	The official who is responsible for the operation and use of an automated information system. (AISSP – Source: DHHS Definition)
System Programmer	A person who develops and maintains system software. (FISCAM)
System Software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software. (FISCAM)
System Testing	Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specification. (FISCAM)
System Security (Computer Security)	Refers to the concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss. (AISSP – Source: FIPS PUB 11-3)
System Security Administrator (SSA)	The person responsible for administering security on a multi-user computer system, communications system, or both.
Systems Security Incidents (Breaches)	Those incidents not classified as physical crimes, criminal violations, fraudulent activity, illegal access and disclosure or misuse of government property. A systems security breach is any action involving a system, which, if not corrected, could violate the provisions of the Privacy Act, Copyright laws, or CMS security policy or lead to a fraudulent act or criminal violation through use of a CMS system.
Systems Security Coordinator (SSC)	Term used to designate the security officer in the 1992 ROM, MIM, and MCM. This Business Partner security officer had complete oversight and responsibility for all aspects of the security of the Medicare program.

Systems Security Officer (SSO)	The position held by the Business Partner Security Officer with complete oversight and responsibility for all aspects of the security of the Medicare program.
System Security Plan (SSP)	Provides a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (AISSP) (OMB Bulletin 90-08)
System Security Profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an information system.
Tape Library	The physical site where magnetic media is stored. (FISCAM)
Tape Management System	Software that controls and tracks tape files. (FISCAM)
Technical Controls	See Logical Access Control.
Telecommunications	A general term for the electronic transmission of information of any type, such as data, television pictures, sound, or facsimiles, over any medium, such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM)
Terminal	A device consisting of a video adapter, a monitor, and a keyboard. (FISCAM)
Threat	(1) Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (NCSC-TG-004) (2) This term defines an event (e.g., a tornado, theft, or computer virus infection), the occurrence of which could have an undesirable impact. (HISM)
Threat Analysis	(1) The examination of all actions and events that might adversely affect a system or operation. (NCSC-TG-004) (2) This task includes the identification of threats that may adversely impact the target environment. (HISM)
Token	In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The token itself is not sufficient; the user must also be able to supply something memorized, such as a personal identification number (PIN). (FISCAM)
Transaction	A discrete activity captured by a computer system, such as an entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records. (FISCAM)
Transaction File	A group of one or more computerized records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods. (FISCAM)

Trap Door	A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with back door. (NCSC-TG-004)
Trojan Horse	(1) A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. (FISCAM) (2) A destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful. (AISSP – Source: Microsoft Press Computer Dictionary)
Unauthorized Disclosure	Exposure of information to individuals not authorized to receive it. (CNSS)
Uncertainty	This term characterizes the degree, expressed as a percent, from 0.0 to 100%, to which there is less than complete confidence in the value of any element of the risk assessment. Uncertainty is typically measured inversely with respect to confidence, i.e., if confidence is low, uncertainty is high. (HISM)
Unclassified	Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (CNSS)
UNIX	A multitasking operating system originally designed for scientific purposes which has subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment. (FISCAM)
Update Access	This access level includes the ability to change data or a software program. (FISCAM)
User	(1) The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) (2) Any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (AISSP – Source: OMB Circular A-130)
User Identification (ID)	A unique identifier assigned to each authorized computer user. (FISCAM)
User Profile	A set of rules that describes the nature and extent of access to each resource that is available to each user. (FISCAM)

Utility Program	Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery). (FISCAM)
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (FISCAM)
Virus	(1) A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. (FISCAM) (2) A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. (NCSC-TG-004)
Vulnerability	(1) This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. Both expected frequency (ARO) and exposure factor (EF) for fire are increased as a consequence of not having a fire suppression system. (HISM) (2) A flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (NIST SP 800-47)
WAN	See Wide Area Network.
Warning Banner	Verbiage that a user sees or is referred to at the point of access to a system which sets the right expectations for users regarding acceptable use of a computer system and its resources, data, and network access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy.
Wide Area Network (WAN)	(1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) (2) A communications network that connects geographically separated areas. (AISSP – Source: Microsoft Press Computer Dictionary)

Workstation	A microcomputer or terminal connected to a network. Workstation can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability. (FISCAM)
Worm	(1) An independent computer Program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. (FISCAM) (2) A program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information. (AISSP – Source: Microsoft Press Computer Dictionary)
Write	Fundamental operation in an information system that results only in the flow of information from a subject to an object. (CNSS)
Write Access	Permission to write to an object in an information system. (CNSS)

Transmittals Issued for this Chapter

Rev #	Issue Date	Subject	Impl Date	CR#
R8SS	04/06/2007	CMS Business Partners System Security Manual	05/01/2007	5500
R7SS	03/17/2006	Self Assessment process in Appendix A and Core Security Requirements	05/01/2006	4342
R6SS	12/09/2005	Incorporation of JSM Instructions in sections 1 through 3	01/09/2006	4111
R5SSS	12/23/2004	Miscellaneous Changes in sections 1 through 3	02/28/2005	3605
R4SSM	03/05/2004	Update links, expand on security concepts, clarify core security requirements and security activities to be conducted/followed, include due dates for system security activities and minor editorial changes.	04/05/2004	3106
R3SSM	03/28/2003	Miscellaneous corrections and clarifications in 1-5 and Appendices	04/11/2003	2568
R2SSM	02/13/2002	Replacement of Manual	02/13/2002	2015
R1SSM	03/28/2003	Initial Issuance of Manual	01/26/2001	1439

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1. Entitywide Security Program Planning and Management

1.1 Management and staff shall receive security training, security awareness, and have security expertise.

1.1.1 Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).

References:
ARS: AT-2.CMS-1
ARS: AT-3.0
FISCAM: TSP-4.2.2
HIPAA: 164.308(a)(5)(i)
HIPAA: 164.308(a)(5)(ii)(A)
HIPAA: 164.308(a)(5)(ii)(B)
HIPAA: 164.308(a)(5)(ii)(C)
HIPAA: 164.308(a)(5)(ii)(D)
NIST 800-53: AT-2
NIST 800-53: AT-3
PISP: 4.2.9.2
PISP: 4.2.9.3

Related CSRs: 2.9.7, 2.9.9, 5.12.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A formal program should be established with a policy and a procedure.

Protocols: 1. Examine organizational records or documents to determine if: (i) security awareness instruction is provided to all users; (ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (iii) records include the type of instruction received and the date completed; and (iv) initial and refresher instruction is provided at least annually.
2. Examine security awareness instructional materials to determine if the materials address the specific requirements of the organization and the information systems to which personnel have authorized access.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness and security training controls are implemented.
4. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently conducts security awareness and security training on an ongoing basis.
5. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security awareness and security training controls are documented and the resulting information used to actively improve the control on a continuous basis.

1.1.2 All information system users (i.e., employees, including managers and senior executives, and contractors) are provided basic security awareness and security training prior to being allowed access to CMS sensitive information or data, and security awareness is repeated when required by system changes, and minimally, on an annual basis.

References:
ARS: AT-2.0
ARS: AT-3.0
CMS: Directed
FISCAM: TSP-3.3.1
HIPAA: 164.308(a)(5)(i)
IRS 1075: 6.2@1.1
IRS 1075: 6.2@1.2
IRS 1075: 6.2@1.3
IRS 1075: 6.2@1.4
NIST 800-53: AT-2
NIST 800-53: AT-3
PISP: 4.2.9.2
PISP: 4.2.9.3

Related CSRs: 1.4.1, 1.10.1, 2.9.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security awareness and security training should inform personnel, including contractors and other users of information systems that support Medicare claims processing of: (1) the proper rules of behavior while using Medicare claims processing systems and information, and (2) their responsibilities in complying with security policies and procedures. Security awareness and security training is provided before allowing access to any sensitive information or system. Security awareness should be a continuing effort but it should be repeated, minimally, on an annual basis.

Protocols: 1. Examine organizational records or documents to determine if: (i) security awareness instruction is provided to all users; (ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (iii) records include the type of instruction received and the date completed; and (iv) initial and refresher instruction is provided at least annually.
2. Examine security awareness instructional materials to determine if the materials address the specific requirements of the organization and the information systems to which personnel have authorized access.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness and security training controls are implemented.
4. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently conducts security awareness and security training on an ongoing basis.
5. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security awareness and security training controls are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.1 Management and staff shall receive security training, security awareness, and have security expertise.

1.1.3 Security training is provided upon employment, promotion, and is adjusted or customized based on the level of the employee's role and responsibilities (i.e., the necessary security skills and competencies necessary to perform a specific role and responsibility).

References:
ARS: AT-2.0
ARS: AT-3.0
CMS: Directed
NIST 800-53: AT-2
NIST 800-53: AT-3
PISP: 4.2.9.2
PISP: 4.2.9.3

Related CSRs: 3.2.1, 3.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security training for an SSO or system security administrator requires more in-depth security skills and competencies (e.g., security controls, incident response, vulnerabilities, etc.) than a claims entry clerk who only requires basic security training on the proper use of security in relation to the processing of sensitive data (e.g., rules of behavior).

Protocols: 1. Examine organizational records or documents to determine if the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities.
2. Examine organizational records or documents to determine if (i) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) the organization provides initial and refresher training at least annually.
3. Examine the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training control is implemented.
5. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently conducts security training on an ongoing basis.
6. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training control are documented and the resulting information used to actively improve the control on a continuous basis.

1.1.4 The employees acknowledge, in writing or electronically, having received the security and awareness training. A record of the security awareness and security training subject(s) covered is maintained.

References:
ARS: AT-4
CMS: Directed
FISCAM: TSP-4.2.3
NIST 800-53: AT-4
PISP: 4.2.9.4

Related CSRs: 1.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There are several ways of maintaining these records. For example, the topics covered can be placed in an e-mail announcing the employees training and subsequently kept in a file.

Protocols: 1. Examine organizational records or documents to determine if the organization monitors and fully documents basic security awareness training and specific information system security training.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training records control is implemented.
3. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently monitors and documents security training activities on an ongoing basis.
4. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training records control are documented and the resulting information used to actively improve the control on a continuous basis.

1.1.5 Security training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided. The use of peer-to-peer (P2P) file sharing technology is controlled and documented to ensure that P2P technology is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

References:
ARS: SA-6
CMS: Directed
NIST 800-53: SA-6
PISP: 4.1.3.6

Related CSRs: 2.2.11, 3.3.1, 7.1.3, 10.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A security policy should exist, and security training should include, appropriate information regarding copyright protection.

Protocols: 1. Review documentation of policy and training to confirm the protection of copyright information under the terms of the provision of the copyright holder.
2. Examine organizational records or documents to determine if the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software usage restrictions control is implemented.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently enforces software usage restrictions on an ongoing basis.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software usage restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.1 Management and staff shall receive security training, security awareness, and have security expertise.

1.1.6 System access is reviewed during extraordinary personnel circumstances.

References:
ARS: PS-CMS-1.CMS-1
PISP: 4.2.1

Related CSRs: 1.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Screening should be consistent with the criteria established for the sensitivity designation of the assigned position.

Protocols: 1. Review relevant policies and procedures for inclusion of the required process.
2. Review the in-place controls for the individuals specified in this requirement.

1.1.7 Personnel with significant information security roles and responsibilities are required to undergo appropriate information system security training prior to performing assigned duties or being authorized access to CMS networks, systems, and/or applications; and undergo refresher training when required by system changes, and minimally, annually thereafter.

References:
ARS: AT-3.0
NIST 800-53: AT-3
PISP: 4.2.9.3

Related CSRs: 1.9.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The roles and responsibilities of an SSO or system security administrator require more in-depth security training and competencies (e.g., security controls, incident response, vulnerabilities, etc.) than a claims entry clerk who only requires basic security training on the proper use of security in relation to the processing of sensitive data (e.g., rules of behavior).

Protocols: 1. Examine organizational records or documents to determine if the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities.
2. Examine organizational records or documents to determine if (i) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) the organization provides initial and refresher training at least annually.
3. Examine the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training control is implemented.
5. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently conducts security training on an ongoing basis.
6. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training control are documented and the resulting information used to actively improve the control on a continuous basis.

1.2 Management shall ensure that corrective security actions are effectively implemented.

1.2.1 Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis.

References:
ARS: CA-7.CMS-1
FISCAM: TSP-5.2
HIPAA: 164.316(b)(2)(iii)
NIST 800-53: CA-7
PISP: 4.1.4.7

Related CSRs: 1.8.7, 1.12.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A corrective security action would consist of designated safeguards from self-assessments, or similar items, developed as the result of an audit. Use of a designated manager, such as the SSO, to monitor implementation and to review the security configuration controls on a continuing basis would satisfy this requirement. This activity should be documented as an internal memorandum on an annual basis.

Protocols: 1. Review records and policy documentation to verify that security corrective actions have been monitored on a continuing basis.
2. Examine organizational records or documents to determine if the organization monitors the security controls in the information system on an ongoing basis.
3. Examine organizational records or documents to determine if the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.
4. Examine organizational records or documents to determine if the organization: (i) assesses designated security controls in the information system; (ii) analyzes for impact, documents, and reports changes to or deficiencies in the operation of the security controls; and (iii) makes adjustments to the information system security plan and plan of action and milestones, as appropriate.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the continuous monitoring control is implemented.
6. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently monitors the security controls in the information system on an ongoing basis.
7. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the continuous monitoring control are documented and the resulting information used to actively improve the control on a continuous basis.

1.2 Management shall ensure that corrective security actions are effectively implemented.

1.2.2 Budget requests (e.g., Line One funding, safeguards) include the allocation of security resources to adequately protect the system and include the determination of security requirements in mission/business planning.

References:
ARS: SA-2
NIST 800-53: SA-2
PISP: 4.1.3.2

Related CSRs: 4.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The business partner includes the determination of security requirements for information systems in mission/business case planning and establishes a line item for information systems security in programming and budgeting documentation.

Protocols: 1. Examine organizational records or documents to determine if the organization allocates, as part of its capital planning and investment control process, the resources required to adequately protect the information system consistent with NIST SP 800-65.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the allocation of resources control is implemented.
3. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently allocates sufficient resources to protect the information system on an ongoing basis.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the allocation of resources control are documented and the resulting information used to actively improve the control on a continuous basis.

1.2.3 A plan of action and milestones (POA&M) is developed for any information system documented findings and the POA&M is updated and submitted to CMS monthly until all the findings are resolved.

References:
ARS: CA-5.0
NIST 800-53: CA-5
PISP: 4.1.4.5

Related CSRs: 1.9.7, 1.12.5, 3.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The POA&M updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. NIST SP 800-37 provides guidance on the security C&A of information systems. NIST SP 800-30 provides guidance on risk mitigation.

Protocols: 1. Examine organizational records or documents to determine if a POA&M for the information system: (i) exists; (ii) is documented; and (iii) is updated monthly.
2. Examine organizational records or documents to determine if the organization follows the POA&M (i.e., correcting deficiencies and meeting milestones).
3. Examine organizational records or documents to determine if the organization follows the POA&M (i.e., correcting deficiencies and meeting milestones).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the POA&M control is implemented.
5. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently develops and updates a POA&M for the information system on an ongoing basis.
6. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the POA&M control are documented and the resulting information used to actively improve the control on a continuous basis.

1.2.4 Security-related activities affecting the information system are planned and coordinated before conducting such activities in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.

References:
NIST 800-53: PL-6

Related CSRs: 2.2.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises.

Protocols: 1. Examine organizational records or documents to determine if appropriate planning and coordination occur before conducting security-related activities affecting the information system.
2. Interview selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the breath and depth of ongoing security-related activities in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security-related activity planning control is implemented.
4. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently plans and coordinates with appropriate organizational elements prior to initiating security-related activities on an ongoing basis.
5. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security-related activity planning control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.

1.3.1 Business Partners transmitting FTI from a main frame computer to another computer need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission. (This CSR applies only to the COB contractor.)

References:
IRS 1075: 3.3@2.2

Related CSRs: 1.3.8 Applicability: COB

Guidance: Transmission of Federal Tax Information must be accompanied by appropriate records that will determine who released the information and what was released.

Protocols: 1. For a sample of documents being received from the IRS, observe handling of receipt of sensitive information for compliance with established procedures.
2. Review relevant policies and procedures for inclusion of the required logging process elements.
3. Interview responsible individual(s) to confirm understanding of the required procedure.
4. Review disclosure list for entries indicating that the documented process has been followed.

1.3.2 Sensitive information, other than that on magnetic tape files or disclosed as a function of normal claims processing operations (e.g., system processes, mailings, payments, etc.), disclosed outside the CMS Business Partner is recorded on a separate list that includes: (1) to whom the disclosure was made; (2) what was disclosed; (3) why it was disclosed; and (4) when it was disclosed.

References:
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(I)
HIPAA: 164.528(b)(2)
IRS 1075: 3.3@2.1

Related CSRs: 1.4.2, 2.12.2 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This is a key element in controlling information within HIPAA. This needs to address areas such as e-mail and other means of transmission of sensitive information.

Protocols: 1. Interview responsible individual(s) to confirm understanding of the required procedure.
2. Review disclosure list for entries indicating that the documented process has been followed.
3. Review relevant policies and procedures for inclusion of the required logging process elements.
4. Observe transmittal of sensitive information for compliance with established procedures.

1.3.3 Appropriate controls are established for all sensitive data entering or leaving the facility. A system is employed that precludes erroneous or unauthorized transfer of data, regardless of media or format. Include controls that maintain a record of shipping and receipts, and a periodic reconciliation of these records.

References:
ARS: MP-5
CMS: Directed
HIPAA: 164.310(d)(1)
HIPAA: 164.310(d)(2)(iii)
NIST 800-53: MP-2
NIST 800-53: MP-5
PISP: 4.2.7.5

Related CSRs: 2.2.25, 2.2.26 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Control procedures should be documented and defined in a Procedures Manual. Another approach would be to provide periodic training.

A policy and set of procedures should exist allowing for the establishment of records regarding sensitive information.

Protocols: 1. Examine organizational records or documents to determine if the organization restricts the pickup, receipt, transfer, and delivery of information system media (paper and digital) to authorized personnel.
2. Examine the list of personnel that have been authorized for the pickup, receipt, transfer, and delivery of information system media to determine if access is appropriately restricted.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media transport control is implemented.
4. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently transports in a secure manner information system media on an ongoing basis.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media transport control are documented and the resulting information used to actively improve the control on a continuous basis.

1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.

1.3.4 All retired, discarded, or unneeded sensitive data is disposed of in a manner that prevents unauthorized persons from using it. All sensitive data is cleared from storage media before releasing as work tapes or disks. Any magnetic media, compact disk, or hard drive that can not be sanitized for reuse is destroyed. Ensure the destruction of any sensitive information hard copy documents when no longer needed.

References:
ARS: MP-7.CMS-1
CMS: Directed
HIPAA: 164.310(d)(2)(i)
HIPAA: 164.310(d)(2)(ii)
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(i)
IRS 1075: 6.3@7
PISP: 4.2.7.7

Related CSRs: 5.9.11, 5.9.12, 5.9.14

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach assures policies and procedures exist for release and/or destruction of CMS sensitive information. A record should be maintained that verifies who performed the destruction and when sensitive information was destroyed.

Protocols: 1. Review disposal procedures for inclusion of protections against use of retired, discarded, or unneeded sensitive data by unauthorized persons.
2. Review disposal procedures for inclusion of use of approved sanitization procedures before release of any nonvolatile storage devices or media.
3. For a sample of employees, interview to determine that disposal procedures are known and being followed.
4. Review disposal procedures for inclusion of use of approved destruction methods during disposal of hard copy documents that are no longer needed.
5. Verify that the reviewed procedure includes protections against sensitive data becoming available to unauthorized personnel.

1.3.5 Retention procedures are implemented for all CMS sensitive information. Sensitive data and CMS Business Partner records (Part A and Part B claims and benefit check records) are stored on-site. When on-site storage is not available, commercial storage facilities are used that most closely meet Federal standards for agency records centers. (Obtain Federal standards on National Archives Record Administration [36 CFR part 1228 subpart K]).

References:
CMS: Directed
HIPAA: 164.316(b)(2)(i)

Related CSRs: 1.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review retention procedures in relation to CMS PMs. When utilizing commercial storage facilities for off-site storage, ensure that any agreements in place address these Federal standards.

Protocols: 1. Review documents establishing the appropriate retention procedures.
2. By inspection confirm that the specified data and records are stored on-site.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

1.3.6 Sensitive information is never disclosed during disposal unless authorized by statute. Destruction of sensitive information is witnessed by a CMS Business Partner employee. However, a Business Partner may elect to have the destruction certified by a shredding contractor in the absence of Business Partner participation.

References:
HIPAA: 164.308(a)(4)(i)
HIPAA: 164.310(d)(2)(ii)
HIPAA: 164.310(d)(2)(iii)
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(i)
IRS 1075: 8.4@1.1
IRS 1075: 8.4@1.2
IRS 1075: 8.4@1.3
IRS 1075: 8.4@1.4
IRS 1075: 8.4@1.5
IRS 1075: 8.4@1.6

Related CSRs: 1.11.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A formal program should be established with a policy and procedure. Review and update existing policy and procedures for addressing these requirements.

Protocols: 1. Review a sample of destruction records to confirm consistent use of the procedure.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.

1.3.7 Before releasing media containing sensitive information to an individual or contractor not authorized to access sensitive information, care is taken to remove all such sensitive information. The sanitization process includes the removal of all data, labels, marking, and activity records using NSA guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88 (Guidelines for Media Sanitization). Procedures are in place to clear sensitive information and software from computers, memory areas, disks, and other equipment or media before they are disposed of or transferred to another use. The responsibility for clearing information is clearly assigned, and standard forms or a record is used to document that all discarded or transferred items are examined for sensitive information and to verify that this information is cleared before the items are released. Sanitization equipment and procedures are tested periodically to verify their correct performance.

References:
ARS: MA-3.3
ARS: MP-6.0
FISCAM: TAC-3.4
HIPAA: 164.310(d)(1)
HIPAA: 164.310(d)(2)(i)
HIPAA: 164.310(d)(2)(ii)
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(i)
IRS 1075: 5.3@2.3
NIST 800-53: MA-3
NIST 800-53: MP-6
PISP: 4.2.5.3
PISP: 4.2.7.6

Related CSRs: 2.12.2, 2.14.1 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is good practice to review the media destruction procedures. In many cases, standard formatting will not remove sensitive data.
Additionally, a tracking or inventory system is used for the hardware but not the sensitive data residing in the electronic media. An approach to ensuring the sensitive data is cleared from the media is to test and reformat multiple times with an approved formatting technique.

Protocols: 1. Examine organizational records or documents to determine if the organization: (i) sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii)conducts periodic tests of sanitization equipment to ensure correct performance.
2. Examine organizational records or documents to determine if the organization sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse consistent with NIST SP 800-88.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media sanitization and disposal control is implemented.
4. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently applies media sanitization and disposal on an ongoing basis.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media sanitization and disposal control are documented and the resulting information used to actively improve the control on a continuous basis.

1.3.8 Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. FTI is physically destroyed by authorized personnel, or returned to the originator or to the system security administrator. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)

References:
IRS 1075: 6.3@6.1
IRS 1075: 6.3@6.2
IRS 1075: 8.1

Related CSRs: 1.3.1 Applicability: COB

Guidance: A formal security program should be established with a policy and procedure. A good approach when returning FTI information to CMS is to obtain a receipt, and provide a notification which contains when and why the information was obtained, how long and for what reason(s) it was used, and when it was returned so as to make the FTI information usage traceable.

Protocols: 1. Review audit data confirming consistent use of the required procedure.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Confirm by inspection that facility has latest version of IRS Publication 1075.

1.3.9 Destruction methods for sensitive information are as follows: (1) burning - the material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (2) mulching or pulping - all material is reduced to particles one inch or smaller; (3) shredding or disintegrating - paper is shredded in cross-cut shredders to a residue particle size not to exceed 1/32 inch in width (with a 1/64 inch tolerance) by 1/2 inch in length, and microfilm is shredded to 1/35 inch by 3/8 inch strips.

References:
ARS: MP-7.CMS-2
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(i)
PISP: 4.2.7.7

Related CSRs: Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Destruction must be accomplished by burning, pulping, melting, chemical decomposition, mutilation, pulverizing, or shredding to the point of non recognition of the information. Ensure that a policy exists that describes, in detail, the procedures that employees must follow for the applicable method of destruction.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming that destruction is accomplished using one or more of the approved methods.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.

1.3.10 Inventory records of all storage media containing sensitive data must be maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media will be logged in a record that identifies: (1) date received, (2) reel/cartridge control number contents, (3) number of records if available, (4) movement, and (5) if disposed of, the date and method of destruction. Such a record must permit all storage media containing sensitive data (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and recorded.

References:
ARS: MP-3.CMS-1
ARS: MP-5
ARS: MP-CMS-1.CMS-1
CMS: Directed
FISCAM: TAC-3.1.A.6
HIPAA: 164.310(d)(2)(iii)
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(i)
IRS 1075: 3.2@1.3
IRS 1075: 3.2@2.2
IRS 1075: 4.6@3.1
NIST 800-53: MP-2
NIST 800-53: MP-3
NIST 800-53: MP-5
PISP: 4.2.7
PISP: 4.2.7.3
PISP: 4.2.7.5

Related CSRs: 1.5.6, 5.4.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: One method would be to ensure that deposits and withdrawals of tapes and other storage media from the library are authorized and recorded, and that audit records kept as part of inventory management.

Protocols: 1. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media transport control are documented and the resulting information used to actively improve the control on a continuous basis.
2. Examine organizational records or documents to determine if the organization restricts the pickup, receipt, transfer, and delivery of information system media (paper and digital) to authorized personnel.
3. Examine the list of personnel that have been authorized for the pickup, receipt, transfer, and delivery of information system media to determine if access is appropriately restricted.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media transport control is implemented.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently transports in a secure manner information system media on an ongoing basis.

1.3.11 Semiannual inventories of removable storage devices and media containing sensitive information are performed.

References:
IRS 1075: 3.2@2.3

Related CSRs: 6.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This approach helps to ensure that no removable storage devices or media are missing by performing and documenting a physical inventory twice a year.

Protocols: 1. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

1.3.12 Removable storage devices and media containing sensitive information are secured before, during, and after processing, and a proper acknowledgement form is signed and returned to the originator.

References:
IRS 1075: 3.2@1.1

Related CSRs: 2.2.20

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A formal program should be established with a policy and procedure.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming consistent use of the required procedure.

1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.

1.3.13 Whenever possible computer operations are in a secure area with restricted access. Sensitive information is kept locked when not in use. Tape reels, disks, or other media are labeled as CMS Sensitive Information. Any magnetic media or compact disk containing sensitive data is kept in a secured area. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information.

References:
ARS: AC-16.CMS-1
ARS: MP-3.0
ARS: MP-4.CMS-3
CMS: Directed
HIPAA: 164.310(a)(1)
HIPAA: 164.310(c)
HIPAA: 164.312(c)(1)
HIPAA: 164.312(c)(2)
HIPAA: 164.312(e)(2)(i)
IRS 1075: 4.6@1.2
IRS 1075: 4.6@1.5
NIST 800-53: AC-16
NIST 800-53: MP-3
NIST 800-53: MP-4
PISP: 4.2.7.3
PISP: 4.2.7.4
PISP: 4.3.2.16

Related CSRs: 2.2.3, 2.5.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information. When removing sensitive data tapes or other magnetic media from robotic systems, apply CMS sensitive information label(s).

Protocols: 1. Examine organizational records or documents to determine if the organization affixes external labels to removable information storage media indicating the distribution limitations and handling caveats of the information.
2. Examine a sample of storage media to determine if the media are affixed with labels indicating the distribution limitations and handling caveats of the information.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the storage media labeling control is implemented.
4. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently applies storage media labeling on an ongoing basis.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the storage media labeling control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis.

1.4 Owners and users shall be aware of security policies.

1.4.1 Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; (6) assuring that system users, including maintenance personnel, receive security awareness training; (7) implementing procedures to determine that the access of a workforce member to CMS sensitive information is appropriate; and (8) establishing a process for requesting, establishing, issuing, and closing user accounts.

References:
ARS: MA-5.0
ARS: PE-5.CMS-1
HIPAA: 164.308(a)(3)(i)
HIPAA: 164.308(a)(3)(ii)(A)
HIPAA: 164.308(a)(3)(ii)(B)
NIST 800-53: MA-5
NIST 800-53: PE-9
PISP: 4.2.2.9
PISP: 4.2.5.5

Related CSRs: 1.1.2, 1.1.4, 1.8.2, 1.10.2, 2.2.31, 2.8.2, 2.8.6, 3.5.2, 4.2.1,

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information.

Protocols: 1. Review the process for requesting, establishing, issuing, and closing user accounts.
2. Review access and maintenance records, and interview a sample of operating and maintenance personnel, to verify that all maintenance access is recorded, and that all maintenance is performed or supervised by authorized, knowledgeable personnel.
3. Review personnel security records and job descriptions to verify that operating and maintenance personnel have the proper clearances.
4. Review relevant policies and procedures for inclusion of the prescribed features.
5. Review training syllabus for inclusion of the security awareness training.
6. Review a sample of training records to confirm completion of security awareness training.

1.4.2 Reporting Improper Inspections or Disclosures of Sensitive Information - Upon discovery by any employee, the individual making the observation or receiving the information contacts his or her supervisor, who contacts CMS for submission to the appropriate authority.

References:
FISCAM: TAC-4.3.3
HIPAA: 164.308(a)(6)(ii)
IRS 1075: 10.1

Related CSRs: 1.3.2, 1.11.1, 2.1.9, 10.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish procedures to identify apparent security violations and ensure that suspicious activity is investigated and appropriate action taken.

Protocols: 1. For a sample of employees, interview to confirm familiarity with the policy and how to report such improper activity.
2. Review relevant policies for inclusion of this directive.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.4 Owners and users shall be aware of security policies.

1.4.3 Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; (3) rules that describe expected behavior of all with access to the system; and (4) procedures to prevent, detect, contain, and correct security violations. Employees acknowledge availability of these policies in writing or electronically.

References:
ARS: PL-4.CMS-2
ARS: PS-6
FISCAM: TSP-3.3.2
HIPAA: 164.308(a)(1)(i)
NIST 800-53: PL-4
NIST 800-53: PS-6
PISP: 4.1.2.4
PISP: 4.2.1.6

Related CSRs: 1.5.1, 1.9.1, 6.3.7, 6.4.2, 9.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish procedures to distribute the security policies to all necessary personnel, and develop a process to document the receipt by the personnel.

Protocols: 1. Examine organizational records or documents to determine if the organization provides and makes readily available to all information system users a set of rules that describes users responsibilities and expected behavior with regard to information and information system usage.
2. Examine organizational records or documents to determine if the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
3. Examine the rules of behavior to determine if the content is consistent with NIST SP 800-18.
4. Interview selected organizational personnel to determine if they understand the rules of behavior for the information system.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the rules of behavior control is implemented.
6. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the rules of behavior on an ongoing basis.
7. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the rules of behavior control are documented and the resulting information used to actively improve the control on a continuous basis.

1.4.4 Procedures are implemented for employees to follow when they discover a privacy breach or a violation of IS systems security. The procedures stipulate: (1) what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.

References:
ARS: IR-2.0
CMS: Directed
HIPAA: 164.308(a)(6)(i)
HIPAA: 164.308(a)(6)(ii)
HSPD-7: H(25)(b)
NIST 800-53: IR-2
PISP: 4.2.8.2

Related CSRs: 1.6.1, 1.6.2, 1.6.3, 1.6.5, 10.9.1, 10.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to access the CERT WEB site for sample procedures for inclusion.

Protocols: 1. Examine the incident response training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.
2. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response control are documented and the resulting information used to actively improve the control on a continuous basis.

1.4.5 Employees are made aware that company policy prohibits the browsing of sensitive data files for any reason other than Medicare business. Medicare information is not used in the CMS Business Partner's private line of business unless authorized by CMS as consistent with the Privacy Act.

References:
CMS: Directed

Related CSRs: 2.9.1, 10.3.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The employee should have a valid need-to-know to view Medicare data. Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business.

Protocols: 1. For a sample of employees, interview to confirm awareness of, and adherence to this policy.
2. Review relevant policies for inclusion of this directive.

1.4 Owners and users shall be aware of security policies.

1.4.6 Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information. Notify users that: (1) they are accessing a U.S. Government information system; (2) CMS maintains ownership and responsibility for its computer systems; (3) users must adhere to CMS Information Security Policies, Standards, and Procedures; (4) user's usage may be monitored, recorded, and audited; (5) unauthorized use is prohibited and subject to criminal and civil penalties; and (6) the use of the information system establishes user's consent to any and all monitoring and recording of their activities.

References:
ARS: AC-8.CMS-1
CMS: Directed
IRS 1075: 5.1@1.3
NIST 800-53: AC-8
PISP: 4.3.2.8

Related CSRs: 1.4.8, 10.6.2, 10.8.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The logon banner/screen warning banner warns the user that the system processes sensitive information and it is subject to monitoring each time they log on.

Protocols: 1. Examine the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries).
2. Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.

1.4.7 All warning banners were developed and implemented in conjunction with legal counsel. The warning message is displayed on the user's screen until the user takes explicit actions to log on to the information system or cancel the session.

References:
ARS: AC-8.CMS-2
ARS: AC-8.CMS-3
NIST 800-53: AC-8
PISP: 4.3.2.8

Related CSRs: 10.8.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist for developing and implementing warning banners.

Protocols: 1. Examine the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries).
2. Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.
4. Test the system use notification message by accessing the login screen for the information system to determine if it remains on the screen until the user takes explicit actions to log on to the information system.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.

1.4 Owners and users shall be aware of security policies.

1.4.8 If keystroke monitoring is used, users are notified.

References:
ARS: AC-8.CMS-1
NIST 800-53: AC-8
PISP: 4.3.2.8

Related CSRs: 1.4.6, 3.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a policy and procedures on the use and control of keystroke monitoring.

Protocols: 1. Examine the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries).
2. Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.

1.5 Information security responsibilities shall be clearly assigned.

1.5.1 The system security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security roles, responsibilities, and expectations for system and network use are clearly defined for: (1) information resource owners and users; (2) information resources management and data processing personnel; (3) senior management; and (4) security administrators.

References:
ARS: PL-4.CMS-1
FISCAM: TSP-3.2
NIST 800-53: CM-8
NIST 800-53: PL-4
NIST 800-53: PS-6
PISP: 4.1.2.4
PISP: 4.2.1.6

Related CSRs: 1.4.3, 4.7.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that the Rules of Behavior are contained in the SSP and that they clearly define the responsibility of all employees.

Protocols: 1. Review the security plan for inclusion of definition of security responsibilities and expected behavior for at least each of the four specified categories of personnel.
2. Review the security plan for inclusion of the required identification of ownership of each computer-related resource, and of responsibilities for managing access to each of these resources.
3. Examine organizational records or documents to determine if the organization provides and makes readily available to all information system users a set of rules that describes users responsibilities and expected behavior with regard to information and information system usage.
4. Examine organizational records or documents to determine if the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
5. Examine the rules of behavior to determine if the content is consistent with NIST SP 800-18.
6. Interview selected organizational personnel to determine if they understand the rules of behavior for the information system.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the rules of behavior control is implemented.
8. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the rules of behavior on an ongoing basis.
9. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the rules of behavior control are documented and the resulting information used to actively improve the control on a continuous basis.

1.5.2 The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.

References:
ARS: PS-CMS-2.CMS-1
CMS: Directed
FISCAM: TSP-3.1.2
HIPAA: 164.308(a)(2)
PISP: 4.2.1

Related CSRs: 9.6.3, 9.6.4, 9.6.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is to certify or ascertain that the SSO has a CISA, CISSP or other appropriate information security certification.

Protocols: 1. Review documentation verifying that an SSO with the required qualifications is designated at an overall level, and at any subordinate levels designated as appropriate by the Business Partner.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.5 Information security responsibilities shall be clearly assigned.

1.5.3 The SSO is organizationally independent of IS operations. If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.

References:
CMS: Directed

Related CSRs: 1.9.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that the SSO's duties allow him/her to act independent of IS operations. Ensure that all Medicare related actions are cleared through the primary Medicare SSO.

Protocols: 1. Review documentation supporting the required organizational independence.
2. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.
3. If these additional SSO positions exist, review documentation supporting use of the specified process.

1.5.4 The SSO assures compliance with CMS systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with CMS systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by CMS Regional Officer and/or Consortium; (4) maintaining systems security documentation for review by CMS Regional Officer and/or Consortium; (5) consulting with the CCMO's designated security officer on systems security issues when there is a need for guidance or interpretation; (6) keeping up with new/advanced systems security technology; (7) participating in all planning groups, having the responsibility to subject all new systems/installations (and major changes) to the risk assessment process; and (8) making certain that specialists such as auditors, lawyers, and building engineers address security issues before changes are made.

References:
ARS: PS-CMS-2.CMS-1
CMS: Directed
HIPAA: 164.316(b)(2)(iii)
PISP: 4.2.1

Related CSRs: 1.9.2, 3.1.2, 9.6.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is to include these in the SSO's job description.

Protocols: 1. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.
2. Review documentation supporting SSO performance of each of the specified roles and responsibilities.

1.5.5 The SSO in each CMS Business Partner organization is responsible for assisting Application System Managers in selecting and implementing appropriate administrative, physical, and technical safeguards for application systems under development or enhancement.

References:
CMS: Directed

Related CSRs: 6.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is to include these in the SSO's job description.

Protocols: 1. Review relevant policies and procedures for inclusion of identification of the specified roles and responsibilities of this security officer.
2. Review relevant documentation for designation of this security officer.

1.5.6 Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.

References:
FISCAM: TAC-3.1.A.3
HIPAA: 164.308(a)(2)
HIPAA: 164.310(d)(1)
IRS 1075: 3.2@1.2

Related CSRs: 1.3.10, 1.13.7, 2.2.20

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to have the SSO designate specific employees this responsibility.

Protocols: 1. Review documentation supporting designation of this responsibility to specific employees.

1.5 Information security responsibilities shall be clearly assigned.

1.5.7 The SSO assures that: (1) internal controls are incorporated into new ADP information systems; (2) appropriate security controls with associated evaluation/test procedures are developed before any procurement action; (3) system security requirements and evaluation/test procedures are included in RFPs and subcontracts involving Medicare claims processing; and (4) requirements in solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

References:
ARS: SA-4.CMS-1
HIPAA: 164.308(b)(1)
HIPAA: 164.308(b)(4)
HIPAA: 164.314(a)(1)
NIST 800-53: SA-4
PISP: 4.1.3.4

Related CSRs: 1.11.2, 1.11.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: NIST SP 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Protocols: 1. Review contracts, RFPs, and other solicitation documentation for inclusion of the specified requirements.
2. Examine organizational records or documents to determine if system acquisition contracts include security requirements and/or security specifications based on an assessment of risk.
3. Examine organizational records or documents to determine if the organization's acquisition of commercial information technology products is consistent with NIST SP 800-23.
4. Examine organizational records or documents to determine if references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST SP 800-70.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the acquisitions control is implemented.
6. Examine organizational records or documents to determine if acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: (i) required security capabilities; (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.
7. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently includes security requirements and/or security specifications in information system acquisition contracts on an ongoing basis.
8. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the acquisitions control are documented and the resulting information used to actively improve the control on a continuous basis.

1.6 An incident response capability shall be implemented.

1.6.1 The following controls exist to identify and report incidents: (1) security incident procedures; (2) report procedures; (3) response procedures; (4) procedures to regularly review records of information system activity, such as security incident tracking reports; and (5) process to modify incident handling procedures and control techniques after an incident occurs. Automated mechanisms are employed to assist in the reporting of security incidents.

References:
ARS: IR-6.1
HIPAA: 164.308(a)(1)(ii)(D)
HIPAA: 164.308(a)(6)(i)
HSPD-7: H(25)(b)
NIST 800-53: IR-6
PISP: 4.2.8.6

Related CSRs: 1.4.4, 1.9.3, 10.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to sample procedures from the CERT website.

Protocols: 1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.
2. Examine organizational records or documents to determine if the organization promptly reports incident information to appropriate authorities.
3. Examine organizational records or documents (or personnel engaged in incident reporting activities) to determine if personnel are following designated incident reporting procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident reporting control is implemented.
5. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently reports information system incidents on an ongoing basis.
6. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident reporting control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if incident reporting functions are automated.
8. Interview selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident reporting capability.
9. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.6 An incident response capability shall be implemented.

1.6.2 The CMS Business Partner's incident response capability has the following characteristics: (1) an understanding of the CMS Business Partners being served; (2) educated information owners and users that trust the incident handling team; (3) a support resource that offers advice and assistance to users for handling and reporting security incidents; (4) a means of prompt centralized reporting; (5) a means of reporting all incidents that may include Personally Identifiable Information (PII) to the CMS project officer/contractor within one hour of recognition; (6) response team members with the necessary knowledge, skills and abilities; (7) links to other relevant groups; and (8) receipt and response to other pertinent security alerts/advisories. Automated mechanisms are employed to increase the availability of incident response-related information and support.

References:

ARS: IR-7.1
ARS: SI-5.1
CMS: Directed
FISCAM: TSP-3.4
NIST 800-53: IR-6
NIST 800-53: IR-7
NIST 800-53: SI-5
PISP: 4.2.6.5
PISP: 4.2.8.7

Related CSRs: 1.4.4, 1.9.3, 10.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to sample procedures from the CERT website.

Protocols: 1. Examine organizational records or documents (including any logs documenting alerts/advisories) to determine if the organization: (i) receives information system security alerts and advisories; (ii) disseminates the alerts and advisories to appropriate personnel; (iii) takes appropriate actions in response; and (iv) documents the results including the date and time of each action taken.
2. Examine organizational records or documents to determine if the organization promptly reports incident information to appropriate authorities.
3. Examine organizational records or documents (or personnel engaged in incident reporting and support activities) to determine if personnel are following designated incident reporting procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident reporting and incident response assistance controls are implemented.
5. Examine organizational records or documents to determine if the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
6. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently provides incident response support and consistently reports information system incidents on an ongoing basis.
7. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization provides the capability to immediately react and respond to new security alerts and advisories.
8. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response assistance and incident reporting controls are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security alerts and advisories control is implemented.
10. Examine organizational records or documents to determine if incident response support and reporting functions are automated.
11. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently receives and responds to security alerts and advisories for the information system on an ongoing basis.
12. Interview selected organizational personnel with incident response support responsibilities to determine how the automated mechanisms improve the incident response support and reporting capability.
13. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security alerts and advisories control are documented and the resulting information used to actively improve the control on a continuous basis.
14. Test selected automated mechanisms to determine if the mechanisms are operating as intended.
15. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization uses automated mechanisms to automatically disseminate security alerts and advisories to appropriate personnel and how the automated mechanisms are implemented.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.6 An incident response capability shall be implemented.

1.6.3 Relevant security incident information is documented according to CMS Computer Security Incident Handling Procedures. Evidence is preserved through technical means, including secured storage of evidence media and write-protection of evidence media. Sound forensics processes are used in addition to utilities that support legal requirements means. The appropriate chain of custody is determined and followed for forensic evidence once an incident has occurred.

References:
ARS: IR-4.CMS-1
ARS: IR-4.CMS-2
NIST 800-53: IR-4
PISP: 4.2.8.4

Related CSRs: 1.4.4, 1.9.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Protocols: 1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.
2. Examine organizational records or documents to determine if the organization implements an incident handling capability for the information system that includes preparation, detection and analysis, containment, eradication, and recovery.
3. Examine organizational records or documents (or personnel engaged in incident handling activities) to determine if personnel are following designated incident handling procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident handling control is implemented.
5. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently conducts incident handling for the information system on an ongoing basis.
6. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident handling control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if incident handling functions are automated.
8. Interview selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident handling capability.
9. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

1.6.4 The incident response capability includes: (1) providing refresher training on incident response roles and responsibilities of personnel on an annual basis; (2) incorporating simulated events as part of incident response training; and (3) employing automated mechanisms to provide a more thorough and realistic incident response training environment.

References:
ARS: IR-2.0
ARS: IR-2.1
ARS: IR-2.2
NIST 800-53: IR-2
PISP: 4.2.8.2

Related CSRs: 1.9.3, 5.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Protocols: 1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.
2. Examine organizational records or documents to determine if the organization identifies personnel with significant incident response roles and responsibilities and documents those roles and responsibilities.
3. Examine organizational records or documents to determine if: (i) incident response training is provided to personnel with significant incident response roles and responsibilities; (ii) records include the type of incident response training received and the date completed; and (iii) initial and refresher training is provided in accordance with organization-defined frequency, at least annually.
4. Examine the incident response training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response training control is implemented.
6. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently conducts incident response training on an ongoing basis.
7. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response training control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if incident response training events are simulated.
9. Interview selected organizational personnel with incident response responsibilities to determine how simulated events improve the training process.

1.6 An incident response capability shall be implemented.

1.6.5 Security incidents are tracked and documented on an on-going basis. Automated mechanisms are employed to assist in tracking and analyzing security incidents. The incident response capability is tested and/or exercised and documented annually, using reviews, analyses, and simulations. Automated mechanisms are employed to more thoroughly and effectively test and/or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

References:
ARS: IR-3.0
ARS: IR-3.1
ARS: IR-5.1
NIST 800-53: IR-3
NIST 800-53: IR-5
PISP: 4.2.8.3
PISP: 4.2.8.5

Related CSRs: 1.4.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Protocols: 1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.
2. Examine organizational records or documents to determine if the organization tests its incident response capability using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests.
3. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently conducts incident response testing on an ongoing basis.
4. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response testing control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Examine organizational records or documents to determine if the organization tracks and documents information system security incidents on an ongoing basis.
6. Examine organizational records or documents (or personnel engaged in incident monitoring activities) to determine if personnel are following designated incident monitoring procedures.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident monitoring control is implemented.
8. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently tracks and documents information system incidents on an ongoing basis.
9. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently tracks and documents information system incidents on an ongoing basis.
10. Examine organizational records or documents to determine if incident tracking and analysis functions are automated.
11. Interview selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident testing and monitoring capability.
12. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

1.6.6 Vulnerabilities exploited during a security incident are identified, and security safeguards are implemented to reduce risk and vulnerability exploit exposure, including isolation or system disconnect. Automated mechanisms are employed to support the incident handling process.

References:
ARS: IR-4.1
ARS: IR-4.CMS-3
NIST 800-53: IR-4
PISP: 4.2.8.4

Related CSRs: 1.8.4, 10.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Protocols: 1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.
2. Examine organizational records or documents to determine if the organization implements an incident handling capability for the information system that includes preparation, detection and analysis, containment, eradication, and recovery.
3. Examine organizational records or documents (or personnel engaged in incident handling activities) to determine if personnel are following designated incident handling procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident handling control is implemented.
5. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently conducts incident handling for the information system on an ongoing basis.
6. Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident handling control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if incident handling functions are automated.
8. Interview selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident handling capability.
9. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.7 Sensitive data to be protected shall be divided into Security levels as appropriate.

1.7.1 CMS has categorized Medicare claims-related information, FTI, and Privacy Act-protected information at the "High" security impact level in accordance with FIPS 199. This information, as well as all information systems that process, store, and/or transmit such information, are protected at the FIPS 199 "High" security level.

References:
ARS: RA-2
CMS: Directed
FISCAM: TAC-1.1
IRS 1075: 4.1@2
NIST 800-53: RA-2
PISP: 4.1.1.2

Related CSRs: 1.3.5, 2.2.2, 2.2.10, 2.2.11, 2.5.3, 2.7.1, 10.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that a policy and procedure exist to categorize and protect all Medicare sensitive data at the FIPS 199 "High" security impact level (See BPSSM Section 4.0).

Protocols: 1. Sensitive Information Safeguard Requirements verify that the combinations of protection implemented for CMS sensitive data match those specified in the Business Partners Systems Security Manual, Section 4.0.
2. Examine the system security plan to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST SP 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization.
3. Interview selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts security categorizations of the information system on an ongoing basis.
6. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security categorization control are documented and the resulting information used to actively improve the control on a continuous basis.

1.8 Minimum protection standards shall consider local factors.

1.8.1 Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.

References:
ARS: PS-8
HIPAA: 164.308(a)(1)(ii)(A)
HIPAA: 164.308(a)(1)(ii)(B)
HIPAA: 164.308(a)(1)(ii)(C)
HSPD-7: G(24)
NIST 800-53: PS-8
PISP: 4.2.1.8

Related CSRs: 1.9.2, 3.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Protocols: 1. Review relevant policies and procedures for inclusion of the required security management features.
2. Examine organizational records or documents to determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
3. Examine organizational records or documents including signed rules of behavior to determine if the organization defines and conveys the formal sanctions process to organizational personnel.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel sanctions control is implemented.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently employs and monitors personnel sanctions on an ongoing basis.
6. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel sanctions control are documented and the resulting information used to actively improve the control on a continuous basis.

1.8 Minimum protection standards shall consider local factors.

1.8.2 Local Information System risk factors are periodically assessed in accordance with the CMS Business RA Methodology, CMS IS RA Methodology, and NIST SP 800-30. The risk assessment is reviewed and updated annually or whenever significant modifications are made to a system, facility, or network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (policy, procedure, separating duties, security awareness and security training, testing/validating/editing, audit routines, audit records, alarms and fire extinguishing equipment, computer system automatic controls, manual controls, good housekeeping, secure disposal, authorizing/restricting access, relocating operations/equipment/records, modifying building/work environment, backup/encryption, insurance/bonding and maintenance/repair/replacement).

References:

ARS: CA-1.CMS-1
ARS: CA-4.CMS-1
ARS: RA-3.CMS-1
ARS: RA-4
CMS: Directed
FISCAM: TSP-1.1
FISCAM: TSP-5.1.1
HIPAA: 164.308(a)(1)(ii)(A)
HSPD-7: G(24)
NIST 800-53: CA-4
NIST 800-53: RA-3
NIST 800-53: RA-4
PISP: 4.1.1.3
PISP: 4.1.1.4
PISP: 4.1.4.2
PISP: 4.1.4.4

Related CSRs: 1.4.1, 1.9.5, 1.12.3, 2.2.31, 3.1.2, 3.1.3, 3.5.2, 5.9.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Protocols: 1. Examine organizational records or documents to determine if a security certification process is defined that assesses the effectiveness of each security control in the information system for correct implementation, intended operation, and producing the desired outcome with respect to meeting the security requirements for the system.
2. Examine organizational records or documents to determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).
3. Examine organizational records or documents to determine if the risk assessment is updated in accordance with organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.
4. Examine organizational records or documents to determine if the organization employs a security certification process in accordance with NIST SP 800-37 and 800-53A.
5. Examine the risk assessment for the information system to determine if the assessment is consistent with NIST SP 800-30 and 800-95.
6. Examine the risk assessment to determine if the report reflects the latest significant changes to the information system, the facilities where the system resides, or other conditions that may have impacted the security or accreditation status of the system.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment and security certification controls are implemented.
8. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently conducts risk assessments and security certifications on an ongoing basis.
9. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the risk assessment for the information system on an ongoing basis.
10. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security certification control are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment and risk assessment update controls are documented and the resulting information used to actively improve the control on a continuous basis.
12. Examine organizational records or documents to determine if an independent certification agent or certification team conducts the security certification of the information system.

1.8 Minimum protection standards shall consider local factors.

1.8.3 Documentation is available to ensure that sensitivity level and criticality designations have been assigned for each system, and that these designations are commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.

References:
ARS: RA-2
CMS: Directed
NIST 800-53: RA-2
PISP: 4.1.1.2

Related CSRs: 3.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review the BPSSM and apply sensitivity level and criticality designations in accordance with FIPS 199.

Protocols: 1. Review documentation establishing that the required designations have been assigned with the considerations specified.
2. Examine the system security plan to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST SP 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization.
3. Interview selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts security categorizations of the information system on an ongoing basis.
6. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security categorization control are documented and the resulting information used to actively improve the control on a continuous basis.

1.8.4 Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities scanned is prepared for each sensitive system and facility being analyzed. Vulnerability scanning tools and techniques include the capability to readily update the list of vulnerabilities scanned at least quarterly or when significant new vulnerabilities are identified and reported.

References:
ARS: RA-5.0
ARS: RA-5.1
ARS: RA-5.2
NIST 800-53: RA-5
PISP: 4.1.1.5

Related CSRs: 1.6.6, 10.8.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review risk assessment.

Protocols: 1. Examine organizational records or documents to determine if the organization scans for vulnerabilities in the information system on an organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported.
2. Examine the latest vulnerability scanning results to determine if the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans.
3. Examine the latest vulnerability scanning results to determine if patch and vulnerability management is handled in accordance with NIST SP 800-40 (Version 2).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the vulnerability scanning control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts vulnerability scanning of the information system on an ongoing basis.
6. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the vulnerability scanning control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with risk assessment responsibilities to determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.
8. Examine previous vulnerability scan results to ensure that the tools used for vulnerability scanning include the capability to update the list of information system vulnerabilities scanned.
9. Examine organizational records or documents to determine if the organization updates the list of information system vulnerabilities scanned on an organization-defined frequency or when significant new vulnerabilities are identified and reported.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.8 Minimum protection standards shall consider local factors.

1.8.5 The risk assessment considers data sensitivity and integrity and the range of risks to the entity's information systems and its data, including information systems managed/operated by external partners.

References:

ARS: RA-3.CMS-1
FISCAM: TSP-1.1.2
HIPAA: 164.308(a)(1)(ii)(A)
NIST 800-53: RA-3
PISP: 4.1.1.3

Related CSRs: 1.13.11, 2.7.1, 3.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Protocols:
1. Review risk assessment policy for inclusion of the required factors.
2. Examine organizational records or documents to determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).
3. Examine the risk assessment for the information system to determine if the assessment is consistent with NIST SP 800-30 and 800-95.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts risk assessments for the information system on an ongoing basis.
6. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment control are documented and the resulting information used to actively improve the control on a continuous basis.

1.8 Minimum protection standards shall consider local factors.

1.8.6 Facilities housing sensitive and critical resources (i.e., key resources) have been identified and prioritized. All significant threat sources, both natural and manmade, to the physical well-being of sensitive and critical resources have been identified and related risks determined in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Adequate physical security controls have been implemented that are commensurate with the risks and magnitude of physical damage or access. Consideration was given to positioning information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

References:

ARS: PE-3.CMS-2
FISCAM: TAC-3.1.A.1
FISCAM: TAC-3.1.A.2
HSPD-7: D(8)
HSPD-7: E(12)
HSPD-7: F(19)(c)
HSPD-7: H(25)(a)
HSPD-7: J(27)(a)
HSPD-7: J(27)(b)
NIST 800-53: PE-18
NIST 800-53: PE-3
PISP: 4.2.2.3

Related CSRs: 1.9.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Protocols: 1. Review documentation supporting an assessment that all significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.
2. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
3. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
4. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization positions information system components within the facility to minimize potential damage from environmental hazards (e.g., electrical interference, electromagnetic radiation, vandalism, eating, drinking, smoking in the proximity, information leakage due to emanation) and to minimize the opportunity for unauthorized access.
6. Examine the facility where the information system components reside to determine if the organization positions components to minimize potential damage from environmental hazards and to minimize the opportunity for unauthorized access.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that physical access and location of information system components controls are implemented.
8. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently controls physical access to the facility and manages the location of system components to minimize risk on an ongoing basis.
9. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of physical access and location of information system components controls are documented and the resulting information used to actively improve the control on a continuous basis.

1.8 Minimum protection standards shall consider local factors.

1.8.7 Top management initiates prompt actions to correct deficiencies and ensures that corrective actions are effectively implemented. Personnel are designated to assign, track, and update risk mitigation efforts. Designated personnel define and authorize corrective action plans, and monitor corrective action progress. Corrective actions are completed within 30 days for all vulnerabilities identified through risk assessment procedures.

References:
ARS: RA-3.CMS-2
FISCAM: TSP-5.1.4
NIST 800-53: RA-3
PISP: 4.1.1.3

Related CSRs: 1.2.1, 1.12.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is to have senior management approve the corrective action plan and have quarterly updates to the plan.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process, and review documentation supporting consistent prompt action by top management to correct deficiencies.
2. Examine organizational records or documents to determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).
3. Examine the risk assessment for the information system to determine if the assessment is consistent with NIST SP 800-30 and 800-95.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts risk assessments for the information system on an ongoing basis.
6. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment control are documented and the resulting information used to actively improve the control on a continuous basis.

1.8.8 Major systems and applications are approved by the managers whose missions they support. Final risk determinations and related management approvals, and written agreements with program officials on the security controls employed and residual risk are documented and maintained on file. (Such determinations and agreements may be incorporated in the system security plan.)

References:
FISCAM: TSP-1.1.3
FISCAM: TSP-5.1.3
HIPAA: 164.308(a)(1)(ii)(A)

Related CSRs: 3.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Protocols: 1. Confirm by inspection that the required documentation and agreements is on file.
2. Inspect documentation of approval for each major system and application by the specified manager.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.1 Formal security and operational procedures and controls are implemented. Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records. System documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to permit analysis and testing of the controls. System documentation is protected, as required, and made available to authorized personnel only.

References:
ARS: CM-2.CMS-2
ARS: SA-5.1
ARS: SA-5.2
ARS: SA-5.CMS-1
ARS: SA-5.CMS-4
HIPAA: 164.308(a)(1)(ii)(A)
NIST 800-53: CM-2
NIST 800-53: CM-8
NIST 800-53: SA-5
PISP: 4.1.3.5
PISP: 4.2.4.2

Related CSRs: 1.4.3, 1.11.2, 9.8.4, 9.8.5, 10.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Protocols: 1. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
2. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.2 A system security plan has been prepared and approved, in accordance with the CMS SSP Methodology, to cover every application and system categorized as a Major Application (MA) or General Support System (GSS).

Related CSRs: 1.5.4, 1.8.1, 1.12.4, 3.2.3, 3.3.2, 3.4.5, 3.5.2, 3.5.3, 3.5.5, 3.6.2, 3.6.3, 9.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: CA-3.CMS-1
ARS: PL-2.CMS-1
ARS: RA-2.1
ARS: SC-CMS-6.CMS-1
CMS: Directed
NIST 800-53: CA-3
NIST 800-53: PL-2
NIST 800-53: RA-2
PISP: 4.1.1.2
PISP: 4.1.2.2
PISP: 4.1.4.3
PISP: 4.3.4

Guidance: Refer to the CMS System Security Plans Methodology for further guidance.

Protocols: 1. Examine organizational records or documents to determine if the security plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.
2. Examine the SSP to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST SP 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization.
3. Examine organizational records or documents to determine if all external information systems (i.e., information systems outside of the accreditation boundary that are connected to the information system) are identified and all resulting system connections are authorized and approved by appropriate organizational officials.
4. Examine the security plan to determine if the plan is consistent with NIST SP 800-18 and addresses security roles, responsibilities, assigned individuals with contact information, and activities for planning security of the information system.
5. Examine information system connection agreements to determine if the agreements are consistent with NIST SP 800-47.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system connections control is implemented.
7. Interview selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners.
8. Interview selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the security plan and are ready to implement the plan.
9. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently authorizes, monitors, and controls information system connections on an ongoing basis.
10. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the SSP control is implemented.
11. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented.
12. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if organizational officials consistently review and approve the security plan for the information system on an ongoing basis.
13. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information systems connection control are documented and the resulting information used to actively improve the control on a continuous basis.
14. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the SSP control are documented and the resulting information used to actively improve the control on a continuous basis.
15. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security categorization control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.3 A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties, and (3) covers the topics prescribed by OMB Circular A-130 such as: (a) system/application rules; (b) security awareness and security training; (c) promotes a continuing awareness of information security issues and threats; (d) personnel controls/personnel security; (e) incident response capability; (f) continuity of support/contingency planning; (g) technical security/technical controls; (h) system interconnection/information sharing; and (i) public access controls.

References:

ARS: AT-2.CMS-1
ARS: CA-3.CMS-1
ARS: SA-5.CMS-1
FISCAM: TSP-2.1
HIPAA: 164.308(a)(4)(i)
HIPAA: 164.310(a)(1)
HIPAA: 164.310(a)(2)(i)
HIPAA: 164.310(a)(2)(ii)
HSPD-7: H(25)(b)
NIST 800-53: AT-2
NIST 800-53: CA-3
NIST 800-53: SA-5
PISP: 4.1.3.5
PISP: 4.1.4.3
PISP: 4.2.9.2

Related CSRs: 1.1.7, 1.6.1, 1.6.2, 1.6.3, 1.6.4, 1.8.6, 2.10.5, 6.1.1, 6.3.13, 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Protocols: 1. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
2. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.
7. Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

1.9.4 The following are accomplished and documented: (1) current system configuration documentation, including links to other systems; (2) security configuration documentation; (3) hardware/software installation and maintenance, including patch management, review and testing for security features; (4) inventory records; (5) security testing; and (6) checking for malicious software.

References:

ARS: SA-5.CMS-4
HIPAA: 164.308(a)(5)(ii)(B)
HIPAA: 164.310(a)(2)(iv)
NIST 800-53: SA-5
PISP: 4.1.3.5
PISP: 4.2.4.2

Related CSRs: 2.5.1, 5.9.4, 5.9.9, 5.12.1, 5.12.2, 6.3.15, 6.3.16, 10.7.3, 10.7.4, 10.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that address these control objectives.

Protocols: 1. Review system configuration documentation for inclusion of links to other systems.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
4. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.
6. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
7. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.
9. Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.5 The system security plan is reviewed and updated to reflect current conditions at least annually, or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security.

References:
ARS: PL-3
FISCAM: TSP-2.2
NIST 800-53: PL-3
PISP: 4.1.2.3

Related CSRs: 1.8.2, 1.12.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Protocols: 1. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Examine organizational records or documents to determine if the security plan is updated in accordance with organization-defined frequency.
4. Examine the security plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system security plan update control is implemented.
6. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the security plan for the information system on an ongoing basis.
7. Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security plan update control are documented and the resulting information used to actively improve the control on a continuous basis.

1.9.6 The system security plan documents a security management structure with adequate independence, authority and expertise.

References:
FISCAM: TSP-3.1.1

Related CSRs: 1.5.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Protocols: 1. Review documentation supporting the assertion that the security management structure meets the stated requirements.
2. Verify by inspection that the system security plan contains the required management structure.

1.9.7 Information system continuous monitoring activities include: (1) configuration management; (2) control of information system components; (3) security impact analyses of changes to the system; (4) on-going assessment of security controls; and (5) status reporting.

References:
ARS: CA-7.CMS-1
NIST 800-53: CA-7
PISP: 4.1.4.7

Related CSRs: 1.2.3, 10.2.9, 10.7.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security monitoring measures should be consistent with NIST SP 800-37.

Protocols: 1. Examine the security control monitoring procedures to determine if the required controls are included.
2. Examine policies and procedures to determine if specific parties are assigned the stated responsibilities.
3. Examine organizational records or documents to determine if the organization monitors the security controls in the information system on an ongoing basis.
4. Examine organizational records or documents to determine if the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.
5. Examine organizational records or documents to determine if the organization: (i) assesses designated security controls in the information system; (ii) analyzes for impact, documents, and reports changes to or deficiencies in the operation of the security controls; and (iii) makes adjustments to the information SSP and POA&M, as appropriate.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the continuous monitoring control is implemented.
7. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently monitors the security controls in the information system on an ongoing basis.
8. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the continuous monitoring control are documented and the resulting information used to actively improve the control on a continuous basis.

1.9.8 A management-initiated independent review or audit of the security controls of all Medicare systems, including interconnected systems, and applications processing sensitive information is performed at least every three years and when a significant change has occurred.

References:
ARS: AC-5.CMS-5
FISCAM: TSP-5.1.2
IRS 1075: 6.3@9.1
PISP: 4.3.2.5

Related CSRs: 1.12.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Periodic independent assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management’s commitment to the security plan.

Protocols: 1. Review documentation verifying independent review includes interconnect system security controls.
2. Review documentation verifying conduct of an independent review or audit at least every three years and when a significant change has occurred.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.9 The CMS Business Partner System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self-assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, CMS, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10) authorization lists that include the designation of the individual responsible for handling security violations and each individual (or position title) responsible for individual assets; and (11) lists of other security records such as audit records and visitor sign-in sheets. Include all other CMS directed or Business Partners System Security Manual directed documents.

References:

ARS: SA-5.CMS-2
ARS: SA-5.CMS-3
CMS: Directed
HIPAA: 164.316(b)(1)
HIPAA: 164.316(b)(2)(ii)
HIPAA: 164.316(b)(2)(iii)
HSPD-7: D(8)
NIST 800-53: SA-5
PISP: 4.1.3.5

Related CSRs: 1.12.7, 2.2.31, 2.2.32, 3.3.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: One method is to incorporate these requirements into the SSO's job description.

Protocols: 1. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
4. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.
6. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
7. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.
9. Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

1.10 Security policies shall exist that address hiring, transfer, termination, and performance.

1.10.1 For prospective employees, references are contacted and background checks performed prior to granting access to CMS sensitive data or systems. Any conditions that allow access prior to completion of the screening process, including the compensating controls that are place, must be documented.

References:

ARS: PS-3.0
CMS: Directed
FISCAM: TSP-4.1.1
NIST 800-53: PS-3
PISP: 4.2.1.3

Related CSRs: 1.1.2, 1.1.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: As part of the HR function, develop a policy and procedure to address hiring, transfer, termination, and performance items.

Protocols: 1. Examine organizational records or documents to determine if the organization appropriately screens individuals requiring access to organizational information and information systems prior to authorizing access.
2. Test the personnel screening process by comparing a list of organizational personnel requiring access to the information system and their associated screening dates to account creation dates to determine if the organization meets the screening criteria for those individuals.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel screening control is implemented.
4. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently conducts personnel screening for positions within the organization on an ongoing basis.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel screening control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.10 Security policies shall exist that address hiring, transfer, termination, and performance.

1.10.2 Regular scheduled vacations exceeding several days and job or shift rotations are required for those personnel using sensitive information.

References:
FISCAM: TSD-1.1.7
FISCAM: TSP-4.1.4
FISCAM: TSP-4.1.5

Related CSRs: 1.4.1, 2.5.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is a policy developed that requires employees using sensitive information to take a minimum of 24 hrs continuous vacation. Personnel whose duties or position gives them access to input or modify sensitive data in such a manner that fraud may be committed should be periodically rotated into different jobs or different shift rotations to introduce other personnel into the process. These rotations increase the likelihood that collaborative fraudulent activities by multiple employees will be disrupted and identified.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of personnel records to confirm compliance with the required vacation policy.
3. Review staff assignment records to confirm that job and shift rotations occur.

1.10.3 Termination and transfer procedures include: (1) exit interview procedures; (2) return of information system-related property (e.g., keys, identification cards, facility passes); (3) notification to security management of terminations and prompt revocation of UserIDs and passwords; (4) providing appropriate personnel with access to official files created by terminated employees; (5) immediately escorting involuntarily terminated employees out of the entity's facilities; and (6) identifying the period during which nondisclosure requirements remain in effect.

References:
ARS: AC-2.CMS-5
ARS: PS-4.CMS-1
ARS: PS-5
FISCAM: TSP-4.1.6
HIPAA: 164.308(a)(3)(ii)(C)
NIST 800-53: AC-2
NIST 800-53: PS-4
NIST 800-53: PS-5
PISP: 4.2.1.4
PISP: 4.2.1.5
PISP: 4.3.2.2

Related CSRs: 2.2.18, 2.9.17, 2.9.18

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: These items need to be addressed as part of a HR Termination/Transfer procedure.

Protocols: 1. Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
2. Examine organizational records or documents to determine if the organization: (i) revokes the information system accounts of terminated personnel; (ii) conducts exit interviews of terminated personnel; (iii) collects all information system-related property (e.g., keys, identification cards, building passes) of terminated personnel; and (iv) retains access to official documents and records on organizational information systems created by terminated personnel.
3. Examine organizational records or documents to determine if the organization: (i) reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and (ii) initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.
4. Examine a list of recently separated or terminated employees to determine if the organization removed accounts for these individuals according to established procedures and completed any organization-required documentation.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
7. Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.
8. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.
9. Test the personnel transfer procedures of the organization by comparing the information system authorizations of current personnel to the access authorizations of transferred personnel to determine if all personnel have appropriate authorizations for the information system.
10. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel termination and transfer controls are implemented.
11. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently manages personnel termination and transfer activities to protect organizational operations and assets on an ongoing basis.
12. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and that appropriate individuals are notified of these occurrences.
13. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel termination and transfer controls are documented and the resulting information used to actively improve the control on a continuous basis.
14. Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.
15. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.10 Security policies shall exist that address hiring, transfer, termination, and performance.

1.10.4 Security is notified immediately when system users are terminated or transferred.

References:
FISCAM: TAC-2.1.6

Related CSRs: 2.2.18, 2.9.17

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Users who continue to have access to critical or sensitive resources pose a major threat, especially those who may have left under acrimonious circumstances.

Protocols: 1. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.
2. Review relevant policies and procedures for inclusion and directed use of the required procedure.

1.10.5 Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.

References:
ARS: PS-3.0
FISCAM: TSP-4.1.2
NIST 800-53: PS-3
PISP: 4.2.1.3

Related CSRs: 2.5.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: CMS will provide future direction.

Protocols: 1. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently conducts personnel screening for positions within the organization on an ongoing basis.
2. Test the personnel screening process by comparing a list of organizational personnel requiring access to the information system and their associated screening dates to account creation dates to determine if the organization meets the screening criteria for those individuals.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel screening control is implemented.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel screening control is implemented.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel screening control are documented and the resulting information used to actively improve the control on a continuous basis.

1.10.6 Signed confidentiality or security agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) are required for CMS Business Partner Medicare employees and their contractors before they are authorized access to any sensitive information system and its related information.

References:
ARS: AC-2.CMS-4
ARS: PL-4.CMS-1
ARS: PL-4.CMS-2
ARS: PS-6
ARS: PS-7.CMS-1
FISCAM: TSP-4.1.3
HIPAA: 164.308(b)(1)
HIPAA: 164.308(b)(4)
HIPAA: 164.314(a)(1)
NIST 800-53: AC-2
NIST 800-53: PL-4
NIST 800-53: PS-6
NIST 800-53: PS-7
PISP: 4.1.2.4
PISP: 4.2.1.6
PISP: 4.2.1.7
PISP: 4.3.2.2

Related CSRs: 1.11.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: One method would be to include the agreements as part of the procedural policy and include a standard contract clause for all procurements.

Protocols: 1. Examine organizational records or documents to determine if the organization: (i) completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access; and (ii) reviews and updates the access agreements on an organization-defined frequency.
2. Examine selected access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for the information system to determine if the access agreements are: (i) signed and retained in accordance with the documented organizational policy and procedures; and (ii) reviewed and updated by the organization on an organization-defined frequency.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access agreements control is implemented.
4. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently completes, reviews, and updates access agreements on an ongoing basis.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access agreements control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.11 Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.

1.11.1 Disclosure of sensitive information is prohibited unless specifically authorized by statute.

References:

CMS: Directed
HIPAA: 164.306(a)(3)
IRS 1075: 11.1@1.1
IRS 1075: 11.1@1.2
IRS 1075: 11.1@1.3
IRS 1075: 11.1@1.4

Related CSRs: 1.3.6, 1.4.2, 1.10.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Examples of statutes that should be reviewed include, but are not limited to, state and federal statutes involving disclosure mandates or restrictions including the HIPAA Privacy Rule, and statutes covering special circumstances.

Protocols: 1. Review relevant policies for inclusion and directed use of the required directive.
2. Review Authorized Disclosure Agreements.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.11 Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.

1.11.2 Written contracts or other arrangements require the inclusion of the CMS Core Security Requirements to protect the integrity, confidentiality, and availability of all information system data. Contractor compliance with CMS information security requirements is monitored to ensure adequate security. The contractor selection process assesses the contractor's ability to adhere to and support CMS' information security policies and standards, as well as all applicable laws, Executive Orders, directives, policies, regulations, and standards. The CMS Business Partner maintains a list of all contracts or other arrangements with other organizations (include organization name and location, contract or agreement number, and purpose). The list of contracts is provided to CMS in an MS Word document with the annual CAST submission.

References:

ARS: AC-2.CMS-4
ARS: AC-6.CMS-3
ARS: PS-7.CMS-1
ARS: SA-4.CMS-1
ARS: SA-9
CMS: Directed
NIST 800-53: PS-7
NIST 800-53: SA-4
NIST 800-53: SA-9
PISP: 4.1.3.4
PISP: 4.1.3.9
PISP: 4.2.1.7
PISP: 4.3.2.2
PISP: 4.3.2.6

Related CSRs: 1.5.7, 1.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A contract between a Business Partner and another organization in which the other organization agrees to electronically exchange data and protect the integrity and confidentiality of the data exchanged should be completed prior to the exchange of any data.

Protocols: 1. Examine organizational records or documents to determine if system acquisition contracts include security requirements and/or security specifications based on an assessment of risk.
2. Examine organizational records or documents to determine if the organization's acquisition of commercial information technology products is consistent with NIST SP 800-23.
3. Examine organizational records or documents to determine if the organization: (i) establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); and (ii) monitors third-party provider compliance to ensure adequate security.
4. Examine organizational records or documents to determine if the organization ensures that third-party providers of information system services employ adequate security controls in the information systems providing such services in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.
5. Examine organizational records or documents to determine if the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST SP 800-35.
6. Examine organizational records or documents to determine if references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST SP 800-70.
7. Interview selected organizational personnel with personnel security responsibilities to determine if the organization monitors third-party provider compliance with personnel security requirements.
8. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the acquisitions control is implemented.
9. Examine organizational records or documents to determine if acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: (i) required security capabilities; (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.
10. Examine the security control assessment results from the organization providing outsourced information system services to determine if the security controls employed by third-party providers are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.
11. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently includes security requirements and/or security specifications in information system acquisition contracts on an ongoing basis.
12. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if third-party providers of information system services consistently employ adequate security controls in the information systems providing those services on an ongoing basis.
13. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the acquisitions control are documented and the resulting information used to actively improve the control on a continuous basis.
14. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the outsourced information system services control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.11 Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.

1.11.3 The CMS Business Partner has obtained satisfactory assurances that all external business associates provide appropriate safeguards for CMS sensitive information. Before issuing external business associates (i.e., contractors, subcontractors) UserIDs to gain access to CMS sensitive systems, written approval is received from the Business Partner CIO or his/her designated representative.

References:
ARS: AC-6.CMS-3
ARS: IA-4.CMS-2
HIPAA: 164.308(b)(1)
HIPAA: 164.314(a)(1)
NIST 800-53: AC-6
NIST 800-53: IA-4
PISP: 4.3.1.4
PISP: 4.3.2.6

Related CSRs: 2.14.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach may be to provide a risk-based solution. All contracts should be part of the security profile and available to the SSO for review.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers.
2. Examine organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
3. Examine organizational records or documents to determine what access rights/privileges the organization assigns to user tasks.
4. Examine selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identifier management control is implemented.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces the most restrictive set of rights/privileges or accesses needed by users on an ongoing basis.
8. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently manages user identifiers for the information system on an ongoing basis.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least privilege control are documented and the resulting information used to actively improve the control on a continuous basis.

1.11.4 Management has authorized connections to all systems (including systems owned and operated by another program, agency, organization, or contractor), and controls have been established and disseminated to the owners of the interconnected systems. A signed Interconnection Security Agreement (ISA) is recorded for each system connection, and remote locations follow all CMS information security policies. System connections are monitored and controlled on an on-going basis. In addition, system connections are recorded in the Information Security (IS) Risk Assessment (RA).

References:
ARS: CA-3.CMS-1
ARS: SC-CMS-6.CMS-1
NIST 800-53: CA-3
PISP: 4.1.4.3
PISP: 4.3.4.1

Related CSRs: 1.13.11, 2.14.2, 10.8.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Appropriate organizational officials should approve information system interconnection agreements. NIST SP 800-47 provides guidance on interconnecting information systems.

Protocols: 1. Examine organizational records or documents to determine if all external information systems (i.e., information systems outside of the accreditation boundary that are connected to the information system) are identified and all resulting system connections are authorized and approved by appropriate organizational officials.
2. Examine information system connection agreements to determine if the agreements are consistent with NIST SP 800-47.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system connections control is implemented.
4. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently authorizes, monitors, and controls information system connections on an ongoing basis.
5. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information systems connection control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.11 Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.

1.11.5 Service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. External providers of information system services are monitored to ensure that they employ adequate security controls in accordance with established service level agreements, and applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

References:

ARS: SA-9.0
NIST 800-53: SA-9
PISP: 4.1.3.9

Related CSRs: 5.7.5, 5.9.1, 5.9.2, 5.10.1, 5.10.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Appropriate organizational officials should approve service level agreements.

Protocols: 1. Examine organizational records or documents to determine if the organization ensures that third-party providers of information system services employ adequate security controls in the information systems providing such services in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.
2. Examine organizational records or documents to determine if the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the outsourced information system services control is implemented.
4. Examine the security control assessment results from the organization providing outsourced information system services to determine if the security controls employed by third-party providers are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if third-party providers of information system services consistently employ adequate security controls in the information systems providing those services on an ongoing basis.
6. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the outsourced information system services control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.11 Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.

1.11.6 Solicitation documents require that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. Appropriate documentation must also be provided that describes the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

References:

NIST 800-53: SA-4

Related CSRs: 1.5.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST SP 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements for information systems categorized in accordance with FIPS 199. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

The information system required documentation also includes security configuration settings and security implementation guidance. NIST SP 800-70 provides guidance on configuration settings for information technology products.

Protocols: 1. Examine organizational records or documents to determine if system acquisition contracts include security requirements and/or security specifications based on an assessment of risk.
2. Examine organizational records or documents to determine if the organization's acquisition of commercial information technology products is consistent with NIST SP 800-23.
3. Examine organizational records or documents to determine if references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST SP 800-70.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the acquisitions control is implemented.
5. Examine organizational records or documents to determine if acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: (i) required security capabilities; (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.
6. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently includes security requirements and/or security specifications in information system acquisition contracts on an ongoing basis.
7. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the acquisitions control are documented and the resulting information used to actively improve the control on a continuous basis.

1.12 Descriptions of Medicare operations, records, and assets are validated once a year.

1.12.1 To provide reasonable assurance that sensitive information is adequately safeguarded, an annual self-assessment is conducted which addresses the safeguard requirements imposed by CMS. A copy of the self-assessment is submitted to CMS.

References:
ARS: CA-2
CMS: Directed
HIPAA: 164.308(a)(8)
HIPAA: 164.316(b)(2)(iii)
IRS 1075: 6.3@1.1
IRS 1075: 6.3@1.2
IRS 1075: 6.3@1.3
IRS 1075: 6.3@1.4
NIST 800-53: CA-2
OMB A-123: (Revised)
PISP: 4.1.4.2

Related CSRs: 1.9.8, 2.5.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that a CISS self-assessment is completed once a year.

Protocols: 1. Review documentation confirming submittal of the most recent self assessment to CMS.
2. Examine organizational records or documents to determine if the security controls in the information system are assessed for correct implementation, for intended operation, and for producing the desired outcome with respect to meeting the security requirements for the system in accordance with organization-defined frequency.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security assessments control is implemented.
4. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization assesses security controls in the information system on an ongoing basis.
5. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security assessments control are documented and the resulting information used to actively improve the control on a continuous basis.

1.12.2 The System Owner/Manager, System Maintainer, or Senior Management designee signs the SSP and certification package. By doing so, they acknowledge the risk to systems under their control and determine the acceptable level of risk.

References:
CMS: Directed

Related CSRs: 2.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review SSP certification package.

Protocols: 1. Inspect the SSP and certification package for the required signatures.

1.12.3 The safeguard selection decisions and the risk assessment reports are carefully analyzed to determine whether the security requirements in place adequately mitigate vulnerabilities. The CMS Business Partner is responsible for approving any necessary corrective action plans.

References:
ARS: RA-3.CMS-2
CMS: Directed
NIST 800-53: RA-3
PISP: 4.1.1.3

Related CSRs: 1.2.1, 1.8.2, 1.8.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review risk assessment and safeguard selection for mitigation of risks and provide recommendations. An approach is to provide annual sign-off, by senior management, on the Corrective Action Plan.

Protocols: 1. Examine organizational records or documents to determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).
2. Examine the risk assessment for the information system to determine if the assessment is consistent with NIST SP 800-30 and 800-95.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment control is implemented.
4. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts risk assessments for the information system on an ongoing basis.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment control are documented and the resulting information used to actively improve the control on a continuous basis.

1.12.4 The CMS Business Partner's systems security certification is completed annually and is fully documented. Whenever new security controls are added, the security controls are tested and the system recertified.

References:
ARS: AC-5.CMS-5
CMS: Directed
PISP: 4.3.2.5

Related CSRs: 1.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation supporting an assertion that the security system is fully documented.
3. Review documentation confirming that the last CMS Business Partner's systems security certification or recertification was completed within the last year or whenever new security controls are added.

1.12 Descriptions of Medicare operations, records, and assets are validated once a year.

1.12.5 A certification assessment of the security controls in the information system is conducted to validate that the controls are implemented correctly, operate as expected, and provide adequate protection in compliance with the security requirements for the information system.

References:
NIST 800-53: CA-4
NIST 800-53: CA-7
PISP: 4.1.4.4
PISP: 4.1.4.7

Related CSRs: 1.2.3, 6.3.2, 10.7.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM.

Protocols: 1. Review documentation confirming that the last CMS Business Partner's systems security certification or recertification was completed within the last year or whenever new security controls are added.
2. Examine organizational records or documents to determine if a security certification process is defined that assesses the effectiveness of each security control in the information system for correct implementation, intended operation, and producing the desired outcome with respect to meeting the security requirements for the system.
3. Examine organizational records or documents to determine if the organization employs a security certification process in accordance with NIST SP 800-37 and 800-53A.
4. Examine organizational records or documents to determine if the organization: (i) assesses designated security controls in the information system; (ii) analyzes for impact, documents, and reports changes to or deficiencies in the operation of the security controls; and (iii) makes adjustments to the information SSP and POA&M, as appropriate.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security certification control is implemented.
6. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently conducts security certifications on an ongoing basis.
7. Examine organizational records or documents to determine if an independent certification agent or certification team conducts the security certification of the information system.

1.12.6 CMS Business Partner office facilities processing sensitive information are subjected to an annual self-assessment.

References:
ARS: CA-2
CMS: Directed
FISCAM: TSP-5.1.1
IRS 1075: 6.3@9.2
NIST 800-53: CA-2
PISP: 4.1.4.2

Related CSRs: 1.9.5, 2.12.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Annual self-assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management’s commitment to the security plan.

Protocols: 1. Examine organizational records or documents to determine if the security controls in the information system are assessed for correct implementation, for intended operation, and for producing the desired outcome with respect to meeting the security requirements for the system in accordance with organization-defined frequency.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security assessments control is implemented.
3. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization assesses security controls in the information system on an ongoing basis.
4. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security assessments control are documented and the resulting information used to actively improve the control on a continuous basis.

1.12.7 Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.

References:
CMS: Directed
HIPAA: 164.316(b)(2)(i)
IRS 1075: 6.3@11.1

Related CSRs: 1.9.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Inspection, self-assessment, and corrective action reports are an important means of identifying areas of noncompliance and remedial actions performed to correct noncompliance.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.13 General workstation security requirements shall be established.

1.13.1 The following workstation security requirements are specified and implemented: (1) what workstation functions can be performed, (2) the manner in which those functions are to be performed, (3) and the physical attributes of the surroundings of a specific workstation or class of workstation that can access CMS sensitive information.

References:
ARS: PE-5.0
HIPAA: 164.310(b)
NIST 800-53: PE-5
PISP: 4.2.2.5

Related CSRs: 7.3.1, 7.3.5, 7.4.1, 7.5.1, 10.6.3, 10.8.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: One approach would be to address all the local workstations as well as the workstations used at home.

Protocols: 1. Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for display medium control is implemented.
3. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently controls physical access to system devices that display information on an ongoing basis.
4. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for display medium control are documented and the resulting information used to actively improve the control on a continuous basis.

1.13.2 Terms and conditions have been established for authorized individuals to: (i) access an information system containing CMS sensitive information from an external information system; and (ii) process, store, and/or transmit CMS sensitive information using an external information system.

References:
ARS: AC-20.0
CMS: Directed
NIST 800-53: AC-20
PISP: 4.3.2.20

Related CSRs: 2.2.23, 6.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Bringing personal computers into the workplace creates vulnerabilities to Medicare resources and could compromise sensitive data.

Protocols: 1. Examine organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions).
2. Interview selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting federal information in accordance with access control policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owed information systems control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs restrictions on the use of personally owned information system on an ongoing basis.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personally owned information systems control are documented and the resulting information used to actively improve the control on a continuous basis.

1.13.3 All CMS-owned software (such as CISS) is secured at close of business or anytime that it is not in use. Manuals and diskettes or CD-ROMs are stored out of sight in desks or file cabinets.

References:
CMS: Directed

Related CSRs: 10.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that address these control objectives.

Protocols: 1. Review audit data confirming enforcement of the required process.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Interview programmers and system manager.

1.13 General workstation security requirements shall be established.

1.13.4 If CMS Business Partner employees are authorized to work on sensitive data at home or an alternate work site, they are required to observe the same security practices that they observe at the office. All appropriate management, operational, and technical information system security controls are employed at the alternate work site.

References:
ARS: AC-20.CMS-1
ARS: PE-17.CMS-1
CMS: Directed
NIST 800-53: AC-20
NIST 800-53: PE-17
PISP: 4.2.2.17
PISP: 4.3.2.20

Related CSRs: 2.2.28

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is to establish policies and procedures that address working "off-site." These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if individuals within the organization employ appropriate information system security controls at alternate work sites.
2. Examine organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions).
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate work site control is implemented.
4. Interview selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting federal information in accordance with access control policy and procedures.
5. Examine the alternate work sites to determine if appropriate information system security controls are in place.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owed information systems control is implemented.
7. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and alternate work sites to determine if individuals within the organization consistently employ appropriate information system security controls at alternate work sites on an ongoing basis.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs restrictions on the use of personally owned information system on an ongoing basis.
9. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate work site control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personally owned information systems control are documented and the resulting information used to actively improve the control on a continuous basis.

1.13.5 Measures are established for controlling the use of laptops, notebooks, and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.

References:
CMS: Directed

Related CSRs: 2.2.28

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An approach is to establish policies and procedures that address working "off-site." These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.

Protocols: 1. Determine the effectiveness of controlling portable devices by review business partner mobile computing policies.

1.13.6 Users are prohibited from installing desktop modems.

References:
ARS: SC-CMS-1.CMS-1
PISP: 4.3.4.1

Related CSRs: 10.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: If no policy currently exists, one should be created. If no process for testing exists, one should be developed.

Protocols: 1. Examine user's desktops for compliance.
2. War-Dialing.
3. Review the policy on addressing desktop modems.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.13 General workstation security requirements shall be established.

1.13.7 The connection of organization-controlled portable computing or portable network devices on the CMS claims processing network is restricted to authorized devices only. Removable hard drives and/or a FIPS-approved method of cryptography are employed to protect information residing on portable and mobile information systems.

References:

ARS: AC-19.1
ARS: PE-CMS-2.CMS-1
ARS: PE-CMS-3.CMS-1
NIST 800-53: AC-19
PISP: 4.2.2.1
PISP: 4.3.2.19

Related CSRs: 1.5.6, 2.5.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.

Protocols: 1. Examine organizational records or documents to determine if: (i) the organization establishes and documents restrictions and implementation guidance for portable and mobile devices; (ii) the organization monitors and controls the use of portable and mobile devices; and (iii) appropriate organizational officials authorize the use of portable and mobile devices and device access to organizational information systems.
2. Interview selected organizational personnel with access to the information system and examine organizational records or documents detailing the use of portable and mobile devices to determine if personnel are complying with the usage restrictions and applying the implementation guidance on the use of portable and mobile devices in accordance with organization policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for portable and mobile devices is implemented.
4. Test the use of portable and mobile devices to access organizational information systems by attempting to connect an unauthorized portable or mobile device to an organizational information system to determine if organizational personnel can identify the unauthorized device.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently implements access controls for portable and mobile devices on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for portable and mobile devices are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization employs removable hard drives or cryptography to protect information on portable and mobile devices.
8. Interview selected organizational personnel who use authorized portable or mobile devices to determine if they employ removable hard drives or cryptography to protect the information on the devices.
9. Examine selected authorized portable or mobile devices to determine if the devices employ removable hard drives or cryptography to protect the information on the devices.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.13 General workstation security requirements shall be established.

1.13.8 The usage of external information systems is prohibited; or, if authorized, their use must adhere to enterprise-wide strict terms and conditions that address the following: (1) types of applications that can be accessed from external information systems; (2) maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (3) prevention of access to federal information on external information system by other users of the system; (4) use of VPN and firewall technologies; (5) use of and protection against the vulnerabilities of wireless technologies; (6) maintenance of adequate physical security controls; (7) use of malicious code and spyware protection software; and (8) installation of and upgrading security capabilities for installed software (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions).

References:

ARS: AC-20.0
NIST 800-53: AC-20
PISP: 4.3.2.20

Related CSRs: 2.2.9, 2.2.24, 5.12.1, 6.2.1, 10.2.2, 10.10.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization (i.e., information systems or components for which the organization typically has no direct control over the application of required security controls), and that are used to process, store, or transmit CMS sensitive information. External information systems include, but are not limited to, personally-owned information systems (e.g., laptop computers, cellular telephones, or personal digital assistants); privately-owned workstations and computing devices resident in hotels, convention centers, or airports; contractor-owned information systems; information systems owned or controlled by other organizations (e.g., support vendors); and other information systems that are not owned by, operated by, or under the direct control of the organization.

Protocols: 1. Examine organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions).
2. Interview selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting federal information in accordance with access control policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owed information systems control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs restrictions on the use of personally owned information system on an ongoing basis.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personally owned information systems control are documented and the resulting information used to actively improve the control on a continuous basis.

1.13 General workstation security requirements shall be established.

1.13.9 Before connecting portable or mobile devices to Medicare claims processing networks, the following is performed: (1) update malicious code protection software; (2) scan for malicious code using approved methods; (3) scan the device for critical software updates and patches; (4) conduct primary operating system integrity checks; and (5) disable unnecessary hardware (e.g., wireless).

References:
NIST 800-53: AC-19

Related CSRs: 2.2.24, 5.12.1, 5.12.2, 10.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a process to review all portable and mobile systems before they are connected to the claims processing network.

Protocols: 1. Examine organizational records or documents to determine if: (i) the organization establishes and documents restrictions and implementation guidance for portable and mobile devices; (ii) the organization monitors and controls the use of portable and mobile devices; and (iii) appropriate organizational officials authorize the use of portable and mobile devices and device access to organizational information systems.
2. Interview selected organizational personnel with access to the information system and examine organizational records or documents detailing the use of portable and mobile devices to determine if personnel are complying with the usage restrictions and applying the implementation guidance on the use of portable and mobile devices in accordance with organization policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for portable and mobile devices is implemented.
4. Test the use of portable and mobile devices to access organizational information systems by attempting to connect an unauthorized portable or mobile device to an organizational information system to determine if organizational personnel can identify the unauthorized device.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently implements access controls for portable and mobile devices on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for portable and mobile devices are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization employs removable hard drives or cryptography to protect information on portable and mobile devices.
8. Interview selected organizational personnel who use authorized portable or mobile devices to determine if they employ removable hard drives or cryptography to protect the information on the devices.
9. Examine selected authorized portable or mobile devices to determine if the devices employ removable hard drives or cryptography to protect the information on the devices.

1.13.10 An automated method is used on demand, and at least weekly, to examine a sample of network systems to determine if unnecessary network services are available. A complete review is performed on demand, and at least monthly.

References:
ARS: CM-7.1
ARS: SC-CMS-2.CMS-1
NIST 800-53: CM-7
PISP: 4.2.4.7
PISP: 4.3.4.1

Related CSRs: 10.8.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish an automated process to examine and review a sample of all connected systems.

Protocols: 1. Examine organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.
2. Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least functionality control is implemented.
4. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies the concept of least functionality to the information system on an ongoing basis.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least functionality control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Category: ***Entitywide Security Program Planning and Management***

General Requirement

Control Technique

1.13 General workstation security requirements shall be established.

1.13.11 Authorized individuals are prohibited from using an external information system to access, process, store, or transmit CMS sensitive information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and SSP; or (ii) there are approved information system connection or processing agreements with the organizational entity hosting the external information system.

References:
NIST 800-53: AC-20

Related CSRs: 1.8.5, 1.11.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally-owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Protocols: 1. Examine organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions).
2. Interview selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting federal information in accordance with access control policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owed information systems control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs restrictions on the use of personally owned information system on an ongoing basis.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personally owned information systems control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: *Access Control*

General Requirement

Control Technique

2. Access Control

2.1 Audit records shall be maintained.

2.1.1 The content of audit records generated by individual components throughout the system is managed centrally. User account activity audits are conducted using automated audit controls. Auditing of administrator activities is enabled and verified.

Related CSRs: 3.1.5, 4.2.2, 9.1.1, 9.1.2, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.8.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AC-13.1
ARS: AC-2.4
ARS: AU-2.0
ARS: AU-2.CMS-2
ARS: AU-3.2
HIPAA: 164.312(b)
NIST 800-53: AC-13
NIST 800-53: AC-2
NIST 800-53: AU-2
NIST 800-53: AU-3
PISP: 4.3.2.13
PISP: 4.3.2.2
PISP: 4.3.3.2
PISP: 4.3.3.3

Guidance: Automated tools support real-time and after-the-fact monitoring. They assist in identifying questionable data access activities, investigating breaches, responding to potential weaknesses, and assessing the security program. Audit reduction tools and/or “intelligent” methods of correlating audit record data may be used to detect unauthorized activity and reduce volumes to manageable size.

Protocols: 1. Interview selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system.
2. Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.
3. Examine organizational records or documents to determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
4. Examine organizational records or documents to determine if unusual activity is investigated, reported to appropriate officials, and resolved.
5. Test the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
6. Examine organizational records of supervisory notices or disciplinary actions to users to determine if the organization is supervising user activities regarding the use and application of information system access controls.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented.
8. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the supervision and review of access control is implemented.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently supervises and reviews user activities with respect to the enforcement and use of access controls for the information system on an ongoing basis.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the supervision and review of access control are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events controls are documented and the resulting information used to actively improve the control on a continuous basis.
12. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities and how those mechanisms are implemented.
13. Interview selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.
14. Examine the information system audit trail to determine if the system accurately compiles audit records from multiple components.
15. Examine the output from the automated mechanism(s) within the information system to determine if each of the automated functions associated with the review of user activities produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.
16. Test the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.
17. Examine organizational records or documents to determine if the information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.
18. Test the information system capability to determine if the content of audit records generated by individual components throughout the system are centrally managed by artificially generating auditable events at different components and utilizing the central management functionality.

2.1 Audit records shall be maintained.

2.1.2 Computer systems processing sensitive information are secured from unauthorized access. All security features are available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing sensitive information is accountable.

References:
ARS: AU-2.0
HIPAA: 164.310(c)
IRS 1075: 5.6@3.3
IRS 1075: 5.6@4.1
NIST 800-53: AU-2
PISP: 4.3.3.2

Related CSRs: 2.2.3, 2.2.21, 2.5.1, 3.1.5, 9.1.1, 9.1.2, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Safeguards are in place to eliminate or minimize the possibility of unauthorized access to sensitive information. The computer systems identified should include those that process Standard Systems, clients used by claims processors, and related computers with sensitive information such as e-mail.

Protocols: 1. Review documentation establishing that the computer systems processing sensitive information are secured from unauthorized access.
2. Review documentation identifying all security features of each hardware and software item in the system, and the extent to which each feature is available and activated.
3. Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.
4. Test the information system by attempting to perform actions that are configured to generate an audit record.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented.
6. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis.
7. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.
9. Examine the information system audit trail to determine if the system accurately compiles audit records from multiple components.
10. Test the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.
11. Examine organizational records or documents to determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.
12. Test the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.

2.1.3 Proper recording of administrator and user account activities, failed and successful logon, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations is enabled.

References:
ARS: AC-13.CMS-2
NIST 800-53: AC-13
PISP: 4.3.2.13

Related CSRs: 2.9.15, 2.9.16

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Maintain, and periodically review, audit records for critical application systems and system events. Audit records may become evidence in legal proceedings, so care should be taken to protect their integrity

Protocols: 1. Interview selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system.
2. Examine organizational records or documents to determine if unusual activity is investigated, reported to appropriate officials, and resolved.
3. Examine organizational records of supervisory notices or disciplinary actions to users to determine if the organization is supervising user activities regarding the use and application of information system access controls.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the supervision and review of access control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently supervises and reviews user activities with respect to the enforcement and use of access controls for the information system on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the supervision and review of access control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities and how those mechanisms are implemented.
8. Examine the configuration of the automated mechanism(s) within the information system to determine if the mechanisms support the review of user activities.
9. Examine the output from the automated mechanism(s) within the information system to determine if each of the automated functions associated with the review of user activities produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.

Category: ***Access Control***

General Requirement

Control Technique

2.1 Audit records shall be maintained.

2.1.4 Privilege restrictions deny non-administrator access to administrator tools, scripts, and utilities. All file system access not explicitly required for system, application, and administrator functionality is disabled.

References:
ARS: AC-6.CMS-1
ARS: AC-6.CMS-2
NIST 800-53: AC-6
PISP: 4.3.2.6

Related CSRs: 2.9.15, 2.9.16, 2.11.2, 3.2.3, 10.7.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Maintain, and periodically review, audit records for critical application systems and system events. Audit records may become evidence in legal proceedings, so care should be taken to protect their integrity

Protocols: 1. Examine organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
2. Examine organizational records or documents to determine what access rights/privileges the organization assigns to user tasks.
3. Examine selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces the most restrictive set of rights/privileges or accesses needed by users on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least privilege control are documented and the resulting information used to actively improve the control on a continuous basis.

2.1.5 All activity involving access to and modifications of sensitive or critical files is recorded.

References:
FISCAM: TAC-4.1

Related CSRs: 3.1.5, 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access control software is used to maintain an audit recordl of security accesses to determine how, when, and by whom specific actions were taken.

In general, the database systems and some transaction systems support this feature. When the critical files are flat files, the feature will require some additional coding.

Protocols: 1. Inspect samples of the specified audit records to confirm continuing use of the required process.
2. Review documentation describing how compliance with this requirement is assured. This should include documentation specifically designating all files considered sensitive or critical, with identification of the corresponding recording methodology for each of these files.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Validate the types of files involved and the features are turned on or coding has been implemented.

Category: ***Access Control***

General Requirement

Control Technique

2.1 Audit records shall be maintained.

2.1.6 Access to audit records is restricted. Audit information and audit tools are protected from unauthorized access, modification, and deletion. Audit functions are not performed by security personnel responsible for administering access control. Automated mechanisms are employed and restricted to hardware-enforced, “write-once” media (e.g., CD-R, not CD-RW) for recording audit information.

References:

ARS: AC-5.CMS-1
ARS: AU-9.1
CMS: Directed
NIST 800-53: AC-5
NIST 800-53: AU-9
PISP: 4.3.2.5
PISP: 4.3.3.9

Related CSRs: 2.10.2, 3.1.5, 9.1.1, 9.1.2, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Computer security managers and system administrators or managers should have read-only access for review purposes; however, security and/or administration personnel who maintain logical access functions should not have access to audit records.

Protocols: 1. Examine organizational records or documents to determine if the information system enforces separation of duties.
2. Examine the information system configuration to determine if the system protects audit information and audit tools from unauthorized access, modification, and deletion.
3. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
4. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
5. Test the protection of audit information and audit tools from unauthorized access, modification, and deletion by attempting to gain unauthorized access, modify, and delete audit information.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties and protection of audit information controls are implemented.
7. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
9. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently protects audit information on an ongoing basis.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties and protection of audit information controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Examine organizational records or documents and the information system configuration to determine if the system produces audit information on hardware-enforced, write-once media.
12. Test the information system to determine if it produces audit information on hardware-enforced, write-once media by executing the process to create the audit information on a write-once media.

Category: ***Access Control***

General Requirement

Control Technique

2.1 Audit records shall be maintained.

2.1.7 The audit record includes sufficient information to establish what events occurred and who or what caused them. The audit record information includes: (1) date and time of the event recorded; (2) component of the information system where the event occurred; (3) type of event; subject identify; and (4) outcome (success or failure) of the event. A capability is provided to compile audit records from multiple components throughout the system into a system-wide (logical or physical) time correlated audit record. Additionally, a capability is provided to manage the selection of events to be audited by individual components of the information system.

References:

ARS: AU-2.1
ARS: AU-2.2
ARS: AU-3.1
CMS: Directed
NIST 800-53: AU-11
NIST 800-53: AU-2
NIST 800-53: AU-3
PISP: 4.3.3.2
PISP: 4.3.3.3

Related CSRs: 3.1.5, 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.3.1, 9.3.3, 9.5.1,

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result. Date and time can help determine if the user was a intruder or the actual person specified.

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.
2. Examine organizational records or documents to determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
3. Examine organizational records or documents to determine if the organization retains information system audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
4. Test the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events and content of audit records controls are implemented.
6. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis.
7. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently captures sufficient audit information to support organizational audit and accountability requirements on an ongoing basis.
8. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events and audit records controls are documented and the resulting information used to actively improve the control on a continuous basis.
9. Interview selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.
10. Examine the information system audit trail to determine if the system accurately compiles audit records from multiple components.
11. Examine organizational records or documents to determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
12. Test the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.
13. Test the information system capability to include additional, more detailed information in the audit records for audit events by changing the audit configuration settings to add additional information and by performing actions that create audit records to ensure the additional information is captured.
14. Examine organizational records or documents to determine if the information system provides the capability to centrally manage the selection of events to be audited and the content of audit records generated by individual components throughout the system.
15. Test the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.
16. Test the information system capability to determine if the content of audit records generated by individual components throughout the system are centrally managed by artificially generating auditable events at different components and utilizing the central management functionality.

2.1 Audit records shall be maintained.

2.1.8 Audit records are generated for the following events: (1) user account management activities; (2) failed and successful logons; (3) security policy modifications; (4) use of administrator privileges; (5) system shutdown; (6) system reboot; (7) system errors; (8) application shutdown; application restart; (9) application errors; (10) file creation; (11) file deletion; (12) file modification; and (13) file access.

References:
ARS: AU-2.0
NIST 800-53: AU-2
PISP: 4.3.3.2

Related CSRs: 10.2.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Maintain, and periodically review, audit records for critical application systems and system events. Audit records may become evidence in legal proceedings, so care should be taken to protect their integrity

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.
2. Test the information system by attempting to perform actions that are configured to generate an audit record.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented.
4. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.
7. Examine the information system audit trail to determine if the system accurately compiles audit records from multiple components.
8. Test the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.
9. Examine organizational records or documents to determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.
10. Test the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.

2.1.9 Disclosures and modifications of personal information, including protected health and financial information are recorded. The record includes: information type, date, time, receiving party, and releasing party. A capability is provided to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. The content of audit records generated by individual components throughout the system is managed centrally.

References:
ARS: AU-3.1
ARS: AU-3.2
ARS: AU-3.CMS-1
HIPAA: 164.528(b)(2)
NIST 800-53: AU-3
PISP: 4.3.3.3

Related CSRs: 1.4.2, 10.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Maintain, and periodically review, audit records for critical application systems, system events, and information disclosures. Audit records may become evidence in legal proceedings, so care should be taken to protect their integrity

Protocols: 1. Examine organizational records or documents to determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Test the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the content of audit records control is implemented.
4. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently captures sufficient audit information to support organizational audit and accountability requirements on an ongoing basis.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the content of audit records control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
7. Test the information system capability to include additional, more detailed information in the audit records for audit events by changing the audit configuration settings to add additional information and by performing actions that create audit records to ensure the additional information is captured.
8. Examine organizational records or documents to determine if the information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.
9. Test the information system capability to determine if the content of audit records generated by individual components throughout the system are centrally managed by artificially generating auditable events at different components and utilizing the central management functionality.

2.1 Audit records shall be maintained.

2.1.10 All hardware fault control routines are recorded to indicate all detected errors and determine if recovery from the malfunction is possible. This information is protected and revealed only to authorized users (e.g., system administrators, maintenance personnel).

References:
ARS: SI-11.0
CMS: Directed
NIST 800-53: SI-11
PISP: 4.2.6.11

Related CSRs: 4.1.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Audit record analysis can often distinguish between operator-induced errors (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code). If a system fails or the integrity of a file (either program or data) is questioned, an analysis of the audit records can reconstruct the series of steps taken by the system, the users, and the application. If a technical problem occurs (e.g., the corruption of a data file) audit records can aid in the recovery process (e.g., by using the record of changes made to reconstruct the file). Correct confirmation of hardware fault routines will provide better recovery techniques and the recorded information will provide better results from hardware maintenance engineers.

Protocols: 1. Determine that audit records have sufficient detail to assist with fault isolation and resolution of security abnormalities.
2. Inspect device configurations to confirm that all detected errors that can be recorded are being recorded.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system establishes a trusted communications path between the user and the security functionality of the system and how the trusted path is implemented.
4. Test the information system trusted path by attempting to establish both a trusted and non-trusted communication path between the user and the security functionality of the system.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the trusted path control is implemented.
6. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently implements a trusted communications path on an ongoing basis.
7. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the trusted path control are documented and the resulting information used to actively improve the control on a continuous basis.

2.1.11 Output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system is retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards; and all applicable NARA requirements. However, they are retained minimally for 90 days, old audit records are archived, and audit record archives retained for one (1) year.

References:
ARS: AU-11.0
ARS: SI-12.1
CMS: Directed
HIPAA: 164.308(a)(1)(ii)(D)
NIST 800-53: AU-11
NIST 800-53: SI-12
PISP: 4.2.6.12
PISP: 4.3.3.11

Related CSRs: 3.1.5, 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 10.3.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Maintain, and periodically review, audit records for critical application systems, including user-written applications. Audit records may become evidence in legal proceedings, so care should be taken to protect their integrity

Protocols: 1. Examine organizational records or documents to determine if the organization retains information system audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
2. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization retains output from the information system in accordance with organizational policy and operational requirements/procedures.
3. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization handles output from the information system in accordance with: (i) labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output; and (ii) organizational policy and operational requirements/procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information output handling and retention control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently handles and retains information output from the information system on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information output handling and retention control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: *Access Control*

General Requirement

Control Technique

2.1 Audit records shall be maintained.

2.1.12 Automated utilities are used to review audit records daily for unusual, unexpected, or suspicious behavior. Manual reviews are performed randomly on demand, but at least once every 30 days. Administrator groups are inspected on demand but at least once every 7 days to ensure unauthorized administrator accounts have not been created.

Related CSRs: 10.2.9, 10.3.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AC-13.CMS-3
ARS: AC-2.0
ARS: AU-6.CMS-4
ARS: AU-6.CMS-5
ARS: AU-6.CMS-6
NIST 800-53: AC-13
NIST 800-53: AC-2
NIST 800-53: AU-6
PISP: 4.3.2.13
PISP: 4.3.2.2
PISP: 4.3.3.6

Guidance: Procedures should exist which describe how to respond to an alert generated by the automated audit record review utilities.

Protocols: 1. Examine organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures.
2. Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation.
3. Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
4. Interview selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
6. Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
8. Examine organizational records of supervisory notices or disciplinary actions to users to determine if the organization is supervising user activities regarding the use and application of information system access controls.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.
11. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.
12. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.
13. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis.
14. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis.
15. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
16. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities and how those mechanisms are implemented.
17. Examine the configuration of the automated mechanism(s) within the information system to determine if the mechanisms support the review of user activities.
18. Examine the output from the automated mechanism(s) within the information system to determine if each of the automated functions associated with the review of user activities produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.
19. Test the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities by artificially generating auditable events and monitoring the results.
20. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.
21. Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.

Category: ***Access Control***

General Requirement

Control Technique

2.1 Audit records shall be maintained.

2.1.13 The information system provides an audit reduction and report generation capability. Audit records are processed automatically for events of interest based upon selected, event criteria. Time stamps generated by internal system clocks that are synchronized system-wide are used in audit record generation.

References:
ARS: AU-7
ARS: AU-8
NIST 800-53: AU-7
NIST 800-53: AU-8
PISP: 4.3.3.7
PISP: 4.3.3.8

Related CSRs: 3.1.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Maintain, and periodically review, audit records for critical application systems and system events. Since audit records may become too large to review, audit reduction tools should be used to capture important and critical audit events. Audit records may become evidence in legal proceedings, so care should be taken to protect their integrity

Protocols: 1. Examine the information system configuration to determine if the system provides time stamps and an audit reduction and report generation capability.
2. Test the audit reduction and report generation capability by artificially generating a sufficient number of auditable events to cause an audit reduction and report generation condition.
3. Test the use of time stamps within the audit record generation capability of the information system by artificially generating an auditable event at a known time and compare the time stamp on the resulting audit record.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the time stamps, audit reduction, and report generation control is implemented.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently provides an audit reduction and report generation capability on an ongoing basis.
6. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently provides time stamps on an ongoing basis.
7. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the time stamps, audit reduction, and report generation control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents and the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.
9. Test the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria by artificially generating auditable events based on selected event criteria.

Category: ***Access Control***

General Requirement

Control Technique

2.1 Audit records shall be maintained.

2.1.14 Sufficient audit record storage capacity is allocated and auditing is configured to provide a warning when allocated capacity reaches ninety percent (90%). In the event of an audit failure or the audit storage capacity being reached, the information system provides a real-time alert to the appropriate officials and takes the additional actions as established by policy (e.g., shutdown the information system, stop generating audit records, overwrite the oldest audit records in the case that storage media is unavailable).

References:

ARS: AU-4
ARS: AU-5.0
ARS: AU-5.1
CMS: Directed
NIST 800-53: AU-4
NIST 800-53: AU-5
PISP: 4.3.3.4
PISP: 4.3.3.5

Related CSRs: 10.2.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish an audit record storage capacity limit and configure the system to prevent exceeding the established limit. The system should be configured to provide a warning and alert appropriate officials when the allocated audit record storage volume reaches 90% of maximum audit record storage capacity. Policy should establish what additional actions should be taken if there is an audit failure or when the audit storage capacity is reached.

Protocols: 1. Examine the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded.
2. Examine the information system configuration to determine if in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions.
3. Test the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded by artificially generating enough auditable events to create a number of audit records to exceed the storage capacity.
4. Test the information system configuration to determine in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions by artificially generating auditable events to cause an audit failure or excess capacity condition.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit storage capacity and audit processing controls are implemented.
6. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently allocates sufficient audit storage capacity on an ongoing basis.
7. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently handles audit processing anomalies including audit failures and exceeding storage capacity on an ongoing basis.
8. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit storage capacity and audit processing controls are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine organizational records or documents and the information system configuration to determine if the system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.
10. Test the information system configuration to determine if the system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity by artificially generating auditable events to cause an excess capacity condition.

Category: *Access Control*

General Requirement

Control Technique

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.1 Procedures are implemented for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges). A record of all physical access, both visitor and authorized individuals is maintained. Management regularly reviews the list of persons with physical access to sensitive facilities. This review is conducted at least once every 30 days.

References:
ARS: PE-2.0
FISCAM: TAC-3.1.A.4
HIPAA: 164.308(a)(3)(i)
HIPAA: 164.310(a)(1)
HIPAA: 164.310(a)(2)(iii)
HIPAA: 164.312(d)
NIST 800-53: PE-2
NIST 800-53: PE-8
PISP: 4.2.2.2

Related CSRs: 2.4.2, 2.8.2, 2.8.6, 10.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures for limiting physical access ensure that properly authorized access is allowed. Access to sensitive facilities should be limited to personnel with a legitimate need for access to perform their duties.

Protocols: 1. Examine organizational records or documents to determine if: (i) the organization develops and keeps current a list of personnel with authorized access to the facility containing the information system; (ii) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (iii) designated officials within the organization review and approve the access list and authorization credentials on an organization-defined frequency.
2. Examine organizational records or documents to determine if the organization maintains a visitor access log to the facility where the information system resides that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; (vii) name and organization of person visited; and (viii) an indication of a designated official's review of the access log within the organization-defined frequency.
3. Examine the facility access list to determine if: (i) the individuals on the list are current personnel assigned to the organization; and (ii) the authorization credentials of the personnel are appropriate.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access authorizations and access log controls are implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization manages physical access authorizations, and maintains and reviews visitor access logs for the facility on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access authorizations control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access logs control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine what automated mechanisms and automated functions are employed to facilitate the maintenance and review of visitor access logs.
9. Examine the automated mechanisms within the facility to determine if each automated function is properly configured to ensure that maintenance and review of visitor access logs are properly performed.

2.2.2 Management analyzes local circumstances to determine space, container, and other security needs at individual facilities that meet or exceed the minimum protection requirements for the FIPS 199 "High" security categorization.

References:
CMS: Directed
IRS 1075: 4.2

Related CSRs: 1.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: See the Business Partners Security Manual for additional information and guidance.

Protocols: 1. Review documentation establishing that a location-specific Risk Analysis was conducted in development of each applicable System Security Plan.

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.3 Access to facilities/data centers is limited to those individuals who routinely need access through the use of guards, identification badges, or physical authentication devices, such as biometrics and/or smart card/PIN combination.

References:
ARS: PE-3.CMS-1
FISCAM: TAC-3.1.A.3
NIST 800-53: PE-3
PISP: 4.2.2.3

Related CSRs: 1.3.13, 2.1.2, 2.5.5, 2.9.3, 2.9.4, 9.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties.

Protocols: 1. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
2. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
3. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls physical access to the facility where the information system resides on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2.4 Physical Intrusion Detection Systems (IDS) are used to provide the security of sensitive information in conjunction with other measures that provide forced entry protection during non-working hours. Automated mechanisms are implemented to ensure that potential physical intrusions are recognized and appropriate actions initiated. Alarms annunciate at an on-site protection console, a central station, or local police station. IDS include, but are not limited to: (1) door and window contacts; (2) magnetic switches; (3) motion detectors; and (4) sound detectors.

References:
ARS: PE-6.1
ARS: PE-6.2
FISCAM: TAC-3.1.A.2
IRS 1075: 4.3@24
NIST 800-53: PE-6
PISP: 4.2.2.6

Related CSRs: 3.6.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Physical security controls used to detect access to facilities and protect them from intentional and unintentional loss or impairment.

Protocols: 1. Examine organizational records, documents, and the facility where the information system resides to determine if the organization monitors physical access to information systems to detect and respond to incidents.
2. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine how individuals respond to physical access incidents.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring physical access control is implemented.
4. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently monitors physical access to the system to detect and respond to incidents on an ongoing basis.
5. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring physical access control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if real-time intrusion alarms and surveillance equipment are used.
7. Examine intrusion alarms and surveillance equipment to determine if the equipment is operational and functioning properly.
8. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate responses.
9. Examine organizational documents or records to determine if physical access intrusions are recognized and appropriate actions initiated.
10. Test the automated mechanisms to determine if each automated function is properly configured to recognize potential intrusions and initiate appropriate responses.

Category: *Access Control*

General Requirement

Control Technique

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.5 Signs denoting restricted areas are prominently posted and separated from non-restricted areas by physical barriers that control access. All entrances have controlled access (e.g., electronic access control, key access, door monitor) and the main entrance to restricted areas is manned. Physical accesses are monitored through audit records and apparent security violations investigated and remedial action taken.

References:

CMS: Directed
IRS 1075: 4.3@3.1
IRS 1075: 4.3@3.2
IRS 1075: 4.3@3.3

Related CSRs: 2.8.3, 5.2.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A restricted area is an area where entry is restricted to authorized personnel. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information. Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a LAN server. The controls can include controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points.

Protocols: 1. Inspect physical access audit records to confirm that the physical accesses are being monitored.
2. Review a sample of audit data confirming consistent use of the required access process.
3. Review documentation describing implementation of the required controls.
4. Review relevant policies and procedures for inclusion and directed use of the required process.

2.2.6 Secured areas/perimeters designed to prevent undetected entry by unauthorized persons during non-working hours are: (1) enclosed by slab-to-slab walls, constructed of approved materials, and supplemented by periodic inspection or other approved protection methods; (2) any lesser-type partition is supplemented by UL-approved electronic intrusion detection and fire detection systems; (3) unless intrusion detection devices are used, all doors entering the space are locked and strict key or combination control is exercised. In the case of a fence and gate, the fence has intrusion detection devices or is continually guarded and the gate is either guarded or locked with intrusion alarms; and (4) the space is cleaned during working hours in the presence of a regularly assigned employee.

References:

ARS: PE-3.CMS-2
CMS: Directed
IRS 1075: 4.3@13.1
NIST 800-53: PE-3
PISP: 4.2.2.3

Related CSRs: 7.3.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The controls over physical access to the elements of a system can include restricted or controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points. Walls forming secured areas should be slab-to-slab or true floor to true ceiling. They should be constructed of substantial materials such as masonry or heavy plywood to prevent the spread of fire and surreptitious entry. The interior walls can be constructed of drywall or plaster board partitions. Review BPSSM Section 4.

Protocols: 1. Review documentation confirming that secured area/perimeters have the required features.
2. Inspect a sample of audit data confirming that the space is cleaned during working hours in the presence of a regularly assigned employee.
3. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
4. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
5. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.
7. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls physical access to the facility where the information system resides on an ongoing basis.
8. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.7 Security rooms, if used, include the following features: (1) entire room is enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection; (2) all doors entering the space are locked with approved locking systems; (3) any glass in doors or walls is security glass (a minimum of two layers of 1/8-inch plate glass with .060-inch [1/32] vinyl interlayer, nominal thickness is 5/16-inch); (4) plastic glazing material is not acceptable; (5) vents and/or louvers are protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station, and is given top priority for guard/police response during any alarm situation; and (6) cleaning and maintenance is performed in the presence of an employee authorized to enter the room.

References:
CMS: Directed
IRS 1075: 4.3@10
IRS 1075: 4.3@11
IRS 1075: 4.3@9.1
IRS 1075: 4.3@9.2
IRS 1075: 4.3@9.3
IRS 1075: 4.3@9.4

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The purpose of security rooms is to store protectable material. Walls forming the perimeter of security rooms should be slab-to-slab or true floor to true ceiling. They should be constructed of substantial materials such as masonry or heavy plywood to prevent the spread of fire and surreptitious entry. The interior walls can be constructed of drywall or plaster board partitions. If security rooms are used, review the requirements in BPSSM Section 4.

Protocols: 1. If Security Rooms are used, review documentation confirming that each includes all of the required features.

2.2.8 Locking Systems for Secured Areas and Security Rooms - High-security pin-tumbler cylinder locks are used that meet the following requirements: (1) key-oriented mortised or rim-mounted deadlock bolt; (2) dead bolt throw of one inch or longer; (3) double-cylinder design; (4) cylinders have five or more pin tumblers; (5) if bolt is visible when locked, it contains hardened inserts or is made of steel; and (6) both the key and the lock are "Off Master." Convenience-type locking devices (e.g., card keys, sequence button-activated locks, etc.) used in conjunction with electric strikes are authorized for use during working hours only. Keys to secured areas are never in personal custody of an unauthorized employee and combinations are stored in a security container.

References:
CMS: Directed
IRS 1075: 4.3@22
IRS 1075: 4.3@23.1
IRS 1075: 4.3@23.3

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security rooms are constructed to resist forced entry and their primary purpose is to store protectable material. Secured areas are interior areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours. The minimum requirements for their locking systems, as stated in this requirement, is contained in BPSSM Section 4. (Also refer to BPSSM Section 4 for additional information on security rooms and secured areas.)

Protocols: 1. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.2.9 Repairs and modifications to security-related physical components of a facility (e.g., hardware, walls, doors, and locks) are documented.

References:
HIPAA: 164.310(a)(2)(iv)

Related CSRs: 1.2.4, 1.13.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is a good practice to keep an inventory of resources.

Protocols: 1. A maintenance tracking system should be implemented.

2.2.10 All restricted areas used to protect sensitive information meet CMS criteria for secured area or security room, or provisions are made to store CMS sensitive information in appropriate security containers during non-working hours.

References:
CMS: Directed
IRS 1075: 4.3@2.2

Related CSRs: 1.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review BPSSM Section 4 for guidance.

Protocols: 1. If Restricted Areas are used to protect sensitive information, review documentation establishing that each meets the specific CMS requirements for either a "Secured Area" or a "Security Room", or that provisions have been made to store CMS sensitive information in appropriate security containers during non-working hours.

2.2.11 CMS Sensitive information in any form is protected during non-working hours through a combination of a secured or locked perimeter, and a secured area or appropriate containerization.

References:
CMS: Directed
IRS 1075: 4.3@1.3

Related CSRs: 1.1.5, 1.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review BPSSM Section 4 for guidance.

Protocols: 1. Review documentation establishing the protective methods and devices employed to protect sensitive information during non-working hours. Confirm use of one or more of the following controls: (1) secured or locked perimeter; (2) secured area; or (3) containerization.
2. Inspect audit data confirming that the required process is consistently used.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.12 Automated mechanisms are employed to control and audit that authorized-only access is permitted to media storage areas that are not protected by guard stations.

References:
ARS: MP-2.1
NIST 800-53: MP-2
PISP: 4.2.7.2

Related CSRs: 2.8.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties.

Protocols: 1. Examine organizational records or documents and/or physical facilities containing media devices to determine if only authorized users have access to information in printed form or on digital media removed from the information system.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media access control is implemented.
3. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently restricts media access on an ongoing basis.
4. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media access control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Examine media storage areas to determine if guard stations control access to media or if automated mechanisms are implemented to control access to media.
6. Examine organizational records or documents to determine if: (i) the organization employs automated mechanisms to ensure only authorized access to media storage areas and to audit access attempts and access granted; and (ii) the types of automated mechanisms and automated functions are configured to ensure only authorized access to such storage areas and to audit access attempts and access granted.
7. Test the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that media access is restricted as required.

2.2.13 Sensitive information (including tapes or cartridges) is placed in secure storage in a secure location, safe from unauthorized access. All containers, rooms, buildings, and facilities containing sensitive information are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.

References:
CMS: Directed
IRS 1075: 4.3@19.2
IRS 1075: 4.3@19.4
IRS 1075: 6.3@4

Related CSRs: 2.13.3, 6.4.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Media controls should be planned for and designed to prevent the loss of confidentiality, integrity, or availability of sensitive information, including data or software, when stored outside the system.

Protocols: 1. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of sensitive information data.
2. Review facility security plan for procedures and policies for protection of sensitive information.

2.2.14 Sensitive information outside secured areas or security rooms during non-working hours is stored in one of the following: (1) metal lateral key-lock files; (2) metal lateral files equipped with lock bars on both sides and secured with security padlocks; (3) metal pull-drawer cabinets with center or off-center lock bars secured by security padlocks; or (4) key-lock "mini safes" properly mounted with appropriate key control.

References:
CMS: Directed
IRS 1075: 4.3@16.1
IRS 1075: 4.3@16.2
IRS 1075: 4.3@16.3
IRS 1075: 4.3@16.3.a
IRS 1075: 4.3@16.3.b
IRS 1075: 4.3@16.3.c
IRS 1075: 4.3@16.3.d

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Sensitive information kept within secured areas or security rooms during non-working hours can be stored in locked containers and do not require a security container. Otherwise, sensitive information must be stored in a security container or safe/vault. (See BPSSM Section 4 for additional information concerning these terms and requirements.)

Protocols: 1. Review documentation supporting the contention that the required process is followed for storage of sensitive information.
2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

2.2.15 If safes and/or vaults are used to store CMS sensitive information outside secure or restricted areas, they comply with: (1) A safe is a GSA-approved container of Class I, IV, and V, or Underwriters Laboratories (UL) listings of TRTL-30, TXTL-60, or TRTL-60; (2) A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, and uses UL-approved vault doors, and meets GSA specifications.

References:
CMS: Directed
IRS 1075: 4.3@18.1
IRS 1075: 4.3@18.2

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Safes and/or vaults are not required for storage of sensitive information if provisions have been made to store CMS sensitive information in other appropriate security containers. However, if they are used, they must meet these GSA/UL requirements as stated in BPSSM Section 4.

Protocols: 1. Examine safe(s) or vault(s) for accompanying manufacturer documentation.

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.16 Locked containers must include lock mechanisms that use either a built-in key, or hasp and lock, and include the following features: (1) metal cabinet or box with riveted or welded seams, or (2) metal desks with locking drawers.

References:
CMS: Directed
IRS 1075: 4.3@15.1
IRS 1075: 4.3@15.2

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A locked container is any metal container which is locked and to which keys and combinations are controlled.

Protocols: 1. Inspect a sample of containers to confirm inclusion of the required features.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.2.17 Keys or other access devices are needed to enter the computer room and tape/media library. Unissued keys or other entry devices are secured.

References:
FISCAM: TAC-3.1.A.5
FISCAM: TAC-3.1.A.7
HIPAA: 164.310(a)(2)(iii)

Related CSRs: 2.8.3, 10.1.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access to these areas should be limited to personnel with a legitimate need for access to perform their duties. Unissued keys and other entry devices should be stored in appropriate security containers.

Protocols: 1. Review documentation confirming implementation and use of the required control.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.

2.2.18 All entry code combinations are changed periodically or when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.

References:
FISCAM: TAC-3.1.B.2
HIPAA: 164.308(a)(3)(ii)(C)
IRS 1075: 4.3@20.3
IRS 1075: 4.3@20.6

Related CSRs: 1.10.3, 1.10.4, 2.9.17

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Periodically changing entry codes prevents reentry by previous employees or visitors who might have knowledge of the entry code. There should be procedures for revoking physical access to controlled areas and removing user accounts when employees terminate employment or when others, such as contractors and vendors, no longer require access.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming consistent use of the required process.
3. Review documentation and records for entry code changes.

2.2.19 Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.

References:
HIPAA: 164.310(c)

Related CSRs: 2.8.3, 3.6.3, 7.3.2, 7.3.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Workstations are located in controlled access areas and are safeguarded from unauthorized access.

Protocols: 1. Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.

2.2.20 Boot access to removable media drives is disabled when not explicitly required. Removable media drives are removed when not explicitly required. If a PC or laptop is not kept or used in a controlled environment, its system BIOS settings are locked and BIOS access is password protected.

References:
ARS: AC-CMS-1.CMS-1
ARS: AC-CMS-1.CMS-2
ARS: AC-CMS-1.CMS-3
CMS: Directed

Related CSRs: 1.3.12, 1.5.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access to removable media drives should be tightly controlled. BIOS access should also be controlled.

Protocols: 1. Review system configuration records.
2. Examine access audit records.
3. Randomly validate BIOS access is protected on desktops.
4. Review documentation on authorized removable media.

2.2.21 Physical ports (e.g., wiring closets, patch panels, etc.) are disabled when not in use.

References:
ARS: PE-CMS-2.CMS-1
PISP: 4.2.2.1

Related CSRs: 2.1.2, 2.3.2, 5.1.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policy should exist which defines the physical ports that are required for operation.

Protocols: 1. Review documentation requiring the disabling of physical ports.

2.2.22 Procedures are implemented to control access to software programs undergoing testing or revision.

References:
HIPAA: 164.310(a)(2)(iii)

Related CSRs: 6.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is good practice to have an Security Test and Evaluation plan.

Protocols: 1. Procedures are in place to protect CMS sensitive information during software testing and revisions.

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.23 Responsibility is assigned and security procedures are implemented for bringing information system hardware and software into and out of the facility, as well as movement of these items within the facility, and for maintaining a record of those items.

References:
ARS: PE-16
HIPAA: 164.310(d)(1)
HIPAA: 164.310(d)(2)(iii)
NIST 800-53: PE-16
PISP: 4.2.2.16

Related CSRs: 1.13.2, 5.4.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The procedures for checking all hardware and software in to and out of the facility assist in maintaining an accurate inventory.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization controls the information system-related items (i.e., hardware, firmware, software) entering and exiting the facility where the system resides and maintains appropriate records of those items.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the delivery and removal control is implemented.
3. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls the delivery and removal of information system-related items from the facility where the system resides on an ongoing basis.
4. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the delivery and removal control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2.24 Transmission and Storage of Data - Sensitive information may be stored on hard disk if the following condition has been met: The CMS Business Partner uses approved security access control devices (hardware/software) that receive regularly scheduled maintenance (including upgrades). Access control devices include: (1) password security; (2) audit records; (3) encryption or guided media; (4) malicious code protection; and (5) data overwriting capabilities. Data stored in the information system must be encrypted when residing in non-secure areas.

References:
ARS: AC-3.CMS-5
CMS: Directed
IRS 1075: 4.7@6.1
IRS 1075: 4.7@6.2
NIST 800-53: AC-3
PISP: 4.3.2.3

Related CSRs: 1.13.8, 1.13.9, 3.6.1, 5.9.5, 5.12.1, 10.3.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The methodology used to ensure confidentiality, both in storage and transmission, can be software based, hardware based, or a combination of both. The robustness of protection provided shall be commensurate with the sensitivity of the information.

Protocols: 1. Examine organizational records or documents to determine if user access to the information system is authorized.
2. Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy.
3. Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling access to the system on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization explicitly defines security functions for the information system.
8. Examine organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy.
9. Test selected accounts that have access to information system security functions to determine if the user privileges for those accounts function as documented in accordance with authorization requirements.

Category: ***Access Control***

General Requirement

Control Technique

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.25 Sensitive information is locked in cabinets or sealed in packing cartons while in transit. Sensitive information material remains in the custody of a CMS or CMS Business Partner employee. Accountability is maintained during the move.

References:

ARS: MP-4.CMS-4
HIPAA: 164.310(d)(2)(iii)
IRS 1075: 4.4
NIST 800-53: MP-4
PISP: 4.2.7.4

Related CSRs: 1.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The policies and procedures for protecting and transferring sensitive information materials with receipts ensure custody control and accountability during transfers.

Protocols: 1. Examine organizational records or documents to determine if the organization protects information system media at the highest FIPS 199 security category for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures.
2. Examine the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media storage control is implemented.
4. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media storage control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2.26 Handling and Transporting Bulk Sensitive Information - Care is taken to safeguard sensitive information at all times. Cryptography is employed to protect information residing on digital media during transport outside of controlled areas. If sensitive information is hand carried between facilities, it is kept with an identified custodian and protected from unauthorized disclosure at all times. All shipments between facilities are documented on transmittal forms and monitored. All bulk shipments transmitted by the U.S. Postal Service, common carrier, or messenger service shall be sent in a sealed, opaque envelope, addressed by name and organization symbol, and marked "To be opened by addressee only."

References:

CMS: Directed
IRS 1075: 4.5
IRS 1075: 4.5@1.1
IRS 1075: 4.5@1.2
IRS 1075: 4.5@2.1
IRS 1075: 4.5@2.2
IRS 1075: 4.5@3.1
NIST 800-53: MP-5

Related CSRs: 1.3.3, 2.5.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: These procedures apply ONLY to the routine and non-routine receipt, handling, and transporting of sensitive information BETWEEN FACILITIES. These requirements are NOT required for routine claims handling and mailings sent from business partners to Medicare recipients.

Protocols: 1. Inspect a sample of sensitive information data media for labeling compliance with the requirement.
2. Examine organizational records or documents to determine if the organization restricts the pickup, receipt, transfer, and delivery of information system media (paper and digital) to authorized personnel.
3. Examine the list of personnel that have been authorized for the pickup, receipt, transfer, and delivery of information system media to determine if access is appropriately restricted.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media transport control is implemented.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently transports in a secure manner information system media on an ongoing basis.
6. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media transport control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.27 Delivery areas are isolated from restricted/controlled areas and are controlled to prevent unauthorized access. Delivery or removal of information system-related items is authorized and controlled by appropriate officials, and records are maintained for the delivery and removal of information system-related items.

References:
ARS: PE-16
NIST 800-53: PE-16
PISP: 4.2.2.16

Related CSRs: 5.9.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization controls the information system-related items (i.e., hardware, firmware, software) entering and exiting the facility where the system resides and maintains appropriate records of those items.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the delivery and removal control is implemented.
3. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls the delivery and removal of information system-related items from the facility where the system resides on an ongoing basis.
4. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the delivery and removal control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2.28 Alternate work site equipment controls include: (1) only CMS Business Partner-owned computers and software are used to process, access, and store sensitive information; (2) a specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with their managers or other members of the Business Partner security staff in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller, Business Partner-owned equipment is locked in a storage cabinet or desk when not in use. If wireless networks are used at alternate work sites, wireless base stations are placed away from outside walls to minimize transmission of data outside of the building.

References:
ARS: AC-20.CMS-1
ARS: PE-17.CMS-1
CMS: Directed
IRS 1075: 4.7@2
IRS 1075: 4.7@3.1
IRS 1075: 4.7@4.1
IRS 1075: 4.7@5.1
IRS 1075: 4.7@5.2
NIST 800-53: AC-20
NIST 800-53: PE-17
PISP: 4.2.2.17
PISP: 4.3.2.20

Related CSRs: 1.13.4, 1.13.5, 10.10.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Employees processing sensitive information at alternate work sites (e.g., home, other contractor or facility) must satisfy these equipment controls to properly protect sensitive information.
An alternate work site is not a hot site. Alternate work sites are those areas where employees, subcontractors, consultants, auditors, etc. perform work associated duties. The most common alternate work site is an employee's home. However, there may be other alternate work sites such as training centers, specialized work areas, processing centers, etc.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if individuals within the organization employ appropriate information system security controls at alternate work sites.
2. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if individuals within the organization employ appropriate information system security controls at alternate work sites.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate work site control is implemented.
4. Examine the alternate work sites to determine if appropriate information system security controls are in place.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and alternate work sites to determine if individuals within the organization consistently employ appropriate information system security controls at alternate work sites on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate work site control are documented and the resulting information used to actively improve the control on a continuous basis.

2.2.29 Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter restricted and other security areas after fire drills or other evacuation procedures.

References:
FISCAM: TAC-3.1.A.8

Related CSRs: 2.8.1, 5.1.5, 5.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Re-entry access methods are used to provide appropriate controls at emergency exits.

Protocols: 1. Inspect a sample of audit data confirming use of the required process.
2. Review written emergency procedures for inclusion of the required process.

Category: ***Access Control***

General Requirement

Control Technique

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.30 Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.

References:
HIPAA: 164.308(a)(3)(i)
HIPAA: 164.310(a)(2)(iii)
IRS 1075: 4.3@1.1

Related CSRs: 2.5.1, 2.5.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Procedures for limiting physical access ensure that properly authorized access is allowed.

Protocols: 1. Review documentation establishing the methods employed to deny access to sensitive information from unauthorized personnel during working hours.
2. If methods used to deny access to sensitive information by unauthorized personnel during working hours do not include use of Restricted Areas, Security Rooms, or Locked Rooms, then review documentation justifying use of alternative methods.

2.2.31 Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.

References:
ARS: MA-5.0
FISCAM: TAC-3.1.B.3
NIST 800-53: MA-5
NIST 800-53: PE-7
PISP: 4.2.5.5

Related CSRs: 1.4.1, 1.8.2, 1.9.9, 5.9.14

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access should be limited to personnel with a legitimate need for access to perform their duties, and they should be controlled and not be granted unrestricted access.

Protocols: 1. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.
2. Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility or areas other than areas designated as publicly accessible.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the visitor control is implemented.
4. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization controls visitor access to the facility on an ongoing basis.
5. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the visitor control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization escorts visitors and monitors visitor activity, when required.

Category: *Access Control*

General Requirement

Control Technique

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.32 Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area records are maintained and include: (1) printed name of visitor and organization; (2) signature of the visitor; (3) form of ID checked; (4) date; (5) time of entry; (6) time of departures; (7) purpose of visit; and (8) printed name of the individual and organization visited. The restricted area record is closed out and reviewed by management at the end of each month. Automated mechanisms are employed to facilitate the maintenance and review of access records. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.

Related CSRs: 1.9.9, 2.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: PE-2.0
ARS: PE-7.1
ARS: PE-8.0
ARS: PE-8.1
FISCAM: TAC-3.1.B.1
HIPAA: 164.308(a)(1)(ii)(D)
HIPAA: 164.310(a)(1)
HIPAA: 164.310(a)(2)(iii)
HIPAA: 164.312(d)
IRS 1075: 4.3@4.1
IRS 1075: 4.3@4.2
IRS 1075: 4.3@6
IRS 1075: 4.3@8.1
IRS 1075: 4.3@8.2
IRS 1075: 4.3@8.3
IRS 1075: 4.3@8.4
NIST 800-53: PE-2
NIST 800-53: PE-7
NIST 800-53: PE-8
PISP: 4.2.2.2
PISP: 4.2.2.7
PISP: 4.2.2.8

Guidance: Persons other than regular authorized personnel may be granted access to sensitive areas or facilities, but these visitors are controlled and not granted unrestricted access.

Protocols: 1. Examine organizational records or documents to determine if: (i) the organization develops and keeps current a list of personnel with authorized access to the facility containing the information system; (ii) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (iii) designated officials within the organization review and approve the access list and authorization credentials on an organization-defined frequency.
2. Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility or areas other than areas designated as publicly accessible.
3. Examine organizational records or documents to determine if the organization maintains a visitor access log to the facility where the information system resides that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; (vii) name and organization of person visited; and (viii) an indication of a designated official's review of the access log within the organization-defined frequency.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the visitor and access record controls are implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization controls visitor access to the facility on an ongoing basis.
6. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently maintains and reviews visitor access logs on an ongoing basis.
7. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization manages physical access authorizations for the facility on an ongoing basis.
8. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the visitor and access record controls are documented and the resulting information used to actively improve the control on a continuous basis.
9. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization escorts visitors and monitors visitor activity, when required.
10. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine what automated mechanisms and automated functions are employed to facilitate the maintenance and review of visitor access logs.
11. Examine the automated mechanisms within the facility to determine if each automated function is properly configured to ensure that maintenance and review of visitor access logs are properly performed.

2.3 Access paths shall be identified.

2.3.1 An analysis of the logical access paths is performed whenever changes to the system are made.

References:
FISCAM: TAC-3.2.B

Related CSRs: 3.4.1, 4.5.1, 10.8.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that all access paths (e.g., Internet, dial-in, telecommunications) be identified and controlled to eliminate "backdoor" paths.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

2.3.2 All access to proxies is denied, except for those hosts, ports, and services that are explicitly required.

References:
ARS: CM-7.1
ARS: SC-7.CMS-2
NIST 800-53: CM-7
NIST 800-53: SC-7
PISP: 4.2.4.7
PISP: 4.3.4.7

Related CSRs: 2.2.21, 10.2.8, 10.8.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Hosts, ports, and services that are required should be explicitly identified.

Protocols: 1. Examine organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.
2. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least functionality control are documented and the resulting information used to actively improve the control on a continuous basis.
3. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies the concept of least functionality to the information system on an ongoing basis.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least functionality and boundary protection controls are implemented.
5. Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.
6. Examine organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.
7. Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

2.3.3 A trusted communications path is established between the user and the security functionality of the system to include at a minimum, information system authentication and reauthentication. The information system provides mechanisms to protect the authenticity of communications sessions.

References:
ARS: SC-11
NIST 800-53: SC-11
NIST 800-53: SC-23
PISP: 4.3.4.11

Related CSRs: 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that only a trusted and controlled communications path be used when setting system security functionality.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system establishes a trusted communications path between the user and the security functionality of the system and how the trusted path is implemented.
2. Test the information system trusted path by attempting to establish both a trusted and non-trusted communication path between the user and the security functionality of the system.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the trusted path control is implemented.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently implements a trusted communications path on an ongoing basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the trusted path control are documented and the resulting information used to actively improve the control on a continuous basis.

2.4 Emergency and temporary access authorization shall be controlled.

2.4.1 Procedures are established (and implemented as needed) that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

References:
HIPAA: 164.310(a)(1)
HIPAA: 164.312(a)(2)(i)
HIPAA: 164.312(a)(2)(ii)

Related CSRs: 2.9.5, 5.2.6, 5.6.3, 6.1.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The mechanism is used to control emergency and temporary access authorizations. Emergency access typically requires unsupervised changes and should require verification and review as part of the procedures.

Protocols: 1. Review documentation of the access control process to confirm inclusion of at least one of the required features.
2. Review documentation of the access control process to confirm inclusion of a procedure for emergency access.

Category: ***Access Control***

General Requirement

Control Technique

2.4 Emergency and temporary access authorization shall be controlled.

2.4.2 Emergency and temporary access authorizations are: (1) documented on standard forms and maintained on file; (2) approved by appropriate managers; (3) securely communicated to the security function; (4) automatically terminated after 15 minutes of no activity; and (5) automatically terminated after a predetermined period.

References:

ARS: AC-2.2
FISCAM: TAC-2.2
NIST 800-53: AC-2
PISP: 4.3.2.2

Related CSRs: 2.2.1, 2.8.2, 5.2.6, 6.1.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: As with normal access authorizations, emergency and temporary access should be approved and documented.

Protocols:
1. Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
2. Examine organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures.
3. Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation.
4. Examine a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.
9. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.
10. Examine organizational records or documents to determine if temporary and emergency accounts are automatically terminated after organization-defined time period for each type of account.
11. Examine the information system configuration settings to determine if the settings are set to automatically terminate temporary and emergency accounts after organization-defined time period.
12. Examine organizational records or documents to determine if any temporary or emergency accounts have not been terminated after organization-defined time period.
13. Test the information system to determine if temporary and emergency accounts are automatically terminated after exceeding a set time period.
14. Examine organizational records or documents to determine if inactive accounts on the information system are automatically disabled after organization-defined time period.
15. Examine the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after organization-defined time period.
16. Examine organizational records or documents to determine if any inactive accounts on the information system have not been disabled after the organization-defined time period, (i.e., if the last login date exceeds the organization-defined time period for disabling inactive accounts).
17. Test the information system to determine if inactive accounts are automatically disabled after exceeding the organization-defined time period.
18. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and that appropriate individuals are notified of these occurrences.
19. Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.

2.5 Resource classifications and related criteria shall be established.

2.5.1 To meet functional and assurance requirements, the operating security features of sensitive information systems must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to sensitive information.

References:
ARS: SA-5.1
CMS: Directed
IRS 1075: 5.7@2.1
IRS 1075: 5.7@2.2
IRS 1075: 5.7@2.3
IRS 1075: 5.7@2.4
NIST 800-53: SA-5
PISP: 4.1.3.5

Related CSRs: 1.9.4, 2.1.2, 2.2.30

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The purpose of security is to support the function of the system, not to undermine it. Therefore, many aspects of the function of the system will produce related security requirements. Assurance documentation can address the security either for a system or for specific components. System-level documentation should describe the system's security requirements and how they have been implemented, including interrelationships among applications, the operating system, or networks. System-level documentation addresses more than just the operating system, the security system, and applications; it describes the system as integrated and implemented in a particular environment. Component documentation will generally be an off-the-shelf product, whereas the system designer or implementer will generally develop system documentation.

Protocols: 1. Review documentation of the configuration management process used to assure that all systems remain in certified configurations.
2. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
3. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
6. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.
8. Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

2.5.2 Every personnel position with access to CMS sensitive information processing is designated with a sensitivity level and risk designation, and the risk designations are reviewed and revised annually. Documentation is available to support the security and suitability standards for these personnel commensurate with their position sensitivity level and appropriate personnel investigation requirements.

References:
ARS: PS-2.0
CMS: Directed
NIST 800-53: PS-2
PISP: 4.2.1.2

Related CSRs: 1.10.2, 1.10.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The staffing process generally involves: (1) defining the job, normally involving the development of a position description; (2) determining the sensitivity level of the position; (3) filling the position, which involves screening applicants and selecting an individual; and (4) security awareness training. The personnel office is normally the first point of contact in helping managers determine if a personnel investigation is necessary for a particular position. See BPSSM Section 2.

Protocols: 1. Examine the organizational records or documents to determine if the organization: (i) establishes risk designations; (ii) assigns a risk designation to all organizational positions; (iii) follows screening criteria for individuals filling organizational positions; and (iv) reviews and revises position risk designations on an organization-defined frequency.
2. Test the position categorization procedures by comparing a list of organizational personnel and their clearance and/or authorization levels to the position risk designations to determine if the organization meets the screening criteria for those individuals filling the positions.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the position categorization control is implemented.
4. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently assigns risk designations for positions within the organization and establishes screening criteria for those positions on an ongoing basis.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the position categorization control are documented and the resulting information used to actively improve the control on a continuous basis.

2.5 Resource classifications and related criteria shall be established.

2.5.3 Classifications and criteria have been established and communicated to resource owners.

References:
ARS: RA-2
FISCAM: TAC-1.1
NIST 800-53: RA-2
PISP: 4.1.1.2

Related CSRs: 1.7.1, 2.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures specifying classification categories and related criteria are established in accordance with Section 4 of the BPSSM to help resource owners classify their resources according to their need for protection controls.

Protocols: 1. Inspect audit data confirming that the required policy has been communicated to resource owners.
2. Examine the SSP to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST SP 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization.
3. Interview selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts security categorizations of the information system on an ongoing basis.
6. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security categorization control are documented and the resulting information used to actively improve the control on a continuous basis.

2.5.4 Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.

References:
HIPAA: 164.308(a)(3)(i)
HIPAA: 164.308(a)(3)(ii)(A)
HIPAA: 164.308(a)(4)(ii)(B)
HIPAA: 164.308(a)(4)(ii)(C)
HIPAA: 164.312(d)
IRS 1075: 6.3@8.a

Related CSRs: 2.2.30, 2.7.2, 2.9.4, 2.12.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures limit access while ensuring that properly authorized access is allowed based on an employee's need-to-know.

Protocols: 1. Review documentation establishing that existing safeguards provide the required protections.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.5 Resource classifications and related criteria shall be established.

2.5.5 Sensitive information is kept separate from other information to the maximum extent possible. If automated information labeling is utilized, information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs/requires special handling). If specific types of media or hardware components are exempted from labeling requirements, they remain within a secure environment and the exemption is authorized in writing by the Business Partner CIO, or his/her designated representative.

Related CSRs: 1.3.13, 1.13.7, 2.2.3, 2.2.26

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AC-16.CMS-1
ARS: MP-3.0
CMS: Directed
IRS 1075: 5.3@1.1
IRS 1075: 5.3@2.1
IRS 1075: 5.3@3.1
IRS 1075: 5.3@3.2
NIST 800-53: AC-16
NIST 800-53: MP-3
NIST 800-53: MP-4
NIST 800-53: MP-5
PISP: 4.2.7.3
PISP: 4.3.2.16

Guidance: Controlling media may require some form of physical labeling. The labels can be used to identify media with special handling instructions, to locate needed information, or to record media (e.g., with serial/control numbers or bar codes) to support accountability. Identification is often by labels on diskettes or tapes or banner pages on printouts.

Protocols:
1. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media labeling and storage controls are documented and the resulting information used to actively improve the control on a continuous basis.
2. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the automated labeling control are documented and the resulting information used to actively improve the control on a continuous basis.
3. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently applies media labeling on an ongoing basis.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently employs an automated labeling capability on an ongoing basis.
5. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media labeling and storage controls are implemented.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the automated labeling control is implemented.
8. Test the automated labeling mechanisms in the information system by displaying selected information in storage, after processing, and after transmission to determine if information is appropriately labeled in accordance with organizational policy and procedures.
9. Examine the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media.
10. Examine the organization-defined list of media types and hardware components that specifies types of media or hardware components that are exempt from labeling so long as they remain within a secure environment.
11. Examine the configuration settings of the information system to determine if the system labels information in storage, in process, and in transmission.
12. Examine organizational records or documents to determine if the organization protects information system media at the highest FIPS 199 security category for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures.
13. Examine organizational records or documents to determine if the organization: (i) affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information; and (ii) exempts specific types of media or hardware components from labeling so long as they remain within a secure environment.
14. Examine a sample of media, both storage media and system output, to determine if the media are affixed with labels indicating the distribution limitations and handling caveats of the information.

2.5 Resource classifications and related criteria shall be established.

2.5.6 Sensitive information system development documentation is available, including security mechanisms and implementation.

References:
ARS: SA-5.2
FISCAM: TCC-1.1.1
NIST 800-53: SA-5
PISP: 4.1.3.5

Related CSRs: 6.3.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The system development documentation provides security mechanism and implementation review guidance to staff with varying levels of skill and experience.

Protocols: 1. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
2. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.
7. Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

2.5.7 Sensitive information system documentation contains the test policy, test plan, test procedures, and retest procedures, and it describes how and what mechanisms were tested, and the results.

References:
FISCAM: TCC-2.1.1
FISCAM: TCC-2.1.4
FISCAM: TCC-2.1.8

Related CSRs: 6.3.7, 6.3.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A disciplined process for testing and approving new and modified systems prior to their implementation is essential to ensure systems operate as intended and that no unauthorized changes are implemented. Security is an integral part of the test.

Protocols: 1. Review the sensitive information system documentation for inclusion of required test documentation.

2.5.8 Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.

References:
CMS: Directed
IRS 1075: 5.6@8

Related CSRs: 1.12.1, 5.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The procedures are used to test the security system attributes.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

Category: ***Access Control***

General Requirement

Control Technique

2.5 Resource classifications and related criteria shall be established.

2.5.9 Security functions are isolated from non-security functions through the use of independent modules in a layered structured (minimizing interactions between layers of the design). Additionally, the security functions for enforcing access and information control are isolated and protected from other security functions and non-security functions.

References:

ARS: SC-3.1
ARS: SC-3.2
ARS: SC-3.3
ARS: SC-3.4
ARS: SC-3.5
NIST 800-53: SC-2
NIST 800-53: SC-3
PISP: 4.3.4.3

Related CSRs: 2.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security functions should be isolated from non-security functions through the use of information system partitions and domains. Separate execution domains (e.g. address space) should be maintained for each executing process. Hardware separation mechanisms should be employed to facilitate the isolation of security functions.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system physically and/or logically separates user functionality (including user interface services) from information system management functionality and how the separation is implemented and enforced.
2. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system isolates security functions from nonsecurity functions (including control of access to and integrity of the hardware, software, and firmware that perform those security functions) and how the system implements and enforces the isolation (e.g., partitions, domains, etc.).
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the application partitioning and security function isolation controls are implemented.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently implements application partitioning on an ongoing basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the application partitioning control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system consistently implements security function isolation on an ongoing basis.
7. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security function isolation control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs hardware separation mechanisms to facilitate security function isolation.
9. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.
10. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.
11. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.
12. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.

Category: ***Access Control***

General Requirement

Control Technique

2.5 Resource classifications and related criteria shall be established.

2.5.10 Users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. System resources shared between two or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

References:

ARS: SC-4.0
HSPD-7: E(12)
NIST 800-53: SC-4
PISP: 4.3.4.4

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that address these control objectives.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system prevents unauthorized and unintended information transfer via shared system resources and how the system prevents the transfer.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information remnants control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs appropriate mechanisms to consistently prevent unauthorized and unintended transfer of information via shared system resources on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information remnants control are documented and the resulting information used to actively improve the control on a continuous basis.

2.6 Actual or attempted unauthorized, unusual, or sensitive access shall be monitored.

2.6.1 Inappropriate or unusual activities or violations with security implications, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. Security personnel are notified and the identified unauthorized, unusual, and sensitive access activities are reported to management, investigated, and appropriate action is taken.

References:
ARS: AU-10
ARS: AU-6.2
ARS: AU-6.CMS-3
ARS: SI-4.CMS-1
FISCAM: TAC-4.2
NIST 800-53: AU-10
NIST 800-53: AU-6
NIST 800-53: SI-4
PISP: 4.2.6.4
PISP: 4.3.3.10
PISP: 4.3.3.6

Related CSRs: 2.9.10, 3.1.1, 4.2.2, 7.1.1, 7.2.2, 7.3.4, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2, 10.2.4, 10.2.6, 10.2.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Audit functions should be activated to maintain critical audit records and report unauthorized or unusual activity to the appropriate personnel.

Protocols: 1. Examine the information system configuration to determine if the system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).
2. Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
3. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools.
4. Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.
6. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system monitoring tools and techniques control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
11. Examine organizational records or documents to determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware.
12. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.

2.6.2 Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.

References:
CMS: Directed

Related CSRs: 3.6.5, 5.2.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Audit records are a mechanism that help managers maintain individual accountability. By advising computer operators that they are personally accountable for their actions, which are tracked by an audit record that records user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be logged in an audit record.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation of the controls used to enforce this requirement.

2.6 Actual or attempted unauthorized, unusual, or sensitive access shall be monitored.

2.6.3 Procedures instruct supervisors: (1) to monitor the activities of visitors to the work area (including CMS Business Partner employees from other work areas); and (2) to ensure that functions of the unit are performed only by employees assigned to the unit. Supervisors shall have procedures for handling questionable activities.

References:
CMS: Directed

Related CSRs: 2.2.32

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Procedures should be in-place to monitor visitors and contractors to insure they perform only authorized activities and work functions.

Protocols: 1. By inspection confirm that supervisors have specified procedures.
2. Confirm by inspection that the required procedures exist.

2.7 Owners of classified resources shall assign adequate classification to documentation and systems.

2.7.1 Resources are classified based on risk assessments. Classifications are documented and approved by an appropriate senior official, and are periodically reviewed.

References:
FISCAM: TAC-1.2
HSPD-7: F(19)(b)

Related CSRs: 1.7.1, 1.8.5, 1.12.2, 2.5.3, 4.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Resource classification determinations flow directly from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing sensitive data or failing to protect the integrity of data supporting critical transactions or decisions.

Protocols: 1. Inspect audit data confirming that the required approval and review processes are consistently used.
2. Review resource classification documentation and compare to risk assessments.

2.7.2 Access to sensitive information is on a strictly need-to-know basis. Contractors evaluate the need for the sensitive information before the data is requested or disseminated.

References:
ARS: MP-4.CMS-4
CMS: Directed
HIPAA: 164.308(a)(4)(i)
HIPAA: 164.308(a)(4)(ii)(C)
HIPAA: 164.308(b)(1)
IRS 1075: 5.2@1.1
IRS 1075: 5.2@1.3
NIST 800-53: MP-4
PISP: 4.2.7.4

Related CSRs: 2.5.4, 2.9.4, 2.12.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The policies and procedures for limiting access ensure that properly authorized access is allowed based on an employee's need-to-know.

Protocols: 1. Examine the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media storage control is implemented.
3. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis.
4. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media storage control are documented and the resulting information used to actively improve the control on a continuous basis.

2.8 Resource owners shall identify authorized users and the level of authorization.

2.8.1 Policy and procedures are implemented for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.

References:
HIPAA: 164.308(a)(3)(i)
HIPAA: 164.312(a)(1)
HIPAA: 164.312(e)(1)

Related CSRs: 2.2.29

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The policies and procedures used to grant different levels of access to sensitive information are based on an employee's need-to-know.

Protocols: 1. Review the appropriate documented policies and procedures for inclusion of the required rules.

2.8 Resource owners shall identify authorized users and the level of authorization.

2.8.2 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to the SSO. Physical access to the information system is controlled independent of the physical access controls for the facility. SSOs or their designated representative review access authorizations and discuss any questionable authorizations with resource owners.

References:
FISCAM: TAC-2.1.1
FISCAM: TAC-2.1.4
NIST 800-53: PE-3

Related CSRs: 1.4.1, 2.2.1, 2.4.2, 2.14.1, 3.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist for authorizing access to information resources and for documenting such authorizations.

Protocols: 1. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
2. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
3. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls physical access to the facility where the information system resides on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access control are documented and the resulting information used to actively improve the control on a continuous basis.

2.8.3 Authorization lists and controls for restricted areas, such as the computer room, tape library, and workstation rooms, are maintained. Authorization lists show the following information: (1) who is authorized access to restricted areas; (2) who is authorized to operate the equipment; (3) which workstations are authorized to access the computer and computer records; and (4) who may maintain operating systems, utilities, and operational versions of application programs.

References:
ARS: PE-2.0
CMS: Directed
NIST 800-53: PE-2
PISP: 4.2.2.2

Related CSRs: 2.2.5, 2.2.12, 2.2.17, 2.2.19, 2.13.3, 6.4.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Authorization lists and controls for restricted areas should be part of doing business to restrict access to areas containing or processing sensitive information.

Protocols: 1. Examine organizational records or documents to determine if: (i) the organization develops and keeps current a list of personnel with authorized access to the facility containing the information system; (ii) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (iii) designated officials within the organization review and approve the access list and authorization credentials on an organization-defined frequency.
2. Examine the facility access list to determine if: (i) the individuals on the list are current personnel assigned to the organization; and (ii) the authorization credentials of the personnel are appropriate.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access authorizations control is implemented.
4. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization manages physical access authorizations for the facility on an ongoing basis.
5. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access authorizations control are documented and the resulting information used to actively improve the control on a continuous basis.

2.8 Resource owners shall identify authorized users and the level of authorization.

2.8.4 All changes to security profiles by SSO or designated representative are automatically recorded and periodically reviewed by management independent of the security function. Unusual activity is investigated.

References:
ARS: AU-6.CMS-6
FISCAM: TAC-2.1.5
NIST 800-53: AU-6
PISP: 4.3.3.6

Related CSRs: 3.1.1, 9.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access controls should be documented, maintained on file, approved by senior managers, and periodically reviewed by resources owners to determine whether they remain appropriate.

Protocols: 1. Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
2. Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.
4. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
7. Test the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities by artificially generating auditable events and monitoring the results.
8. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.
9. Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.

2.8.5 The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners.

References:
FISCAM: TAC-2.1.3

Related CSRs: 5.9.12, 5.9.13, 10.10.1

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Because dial-up access can significantly increase the risk of unauthorized access, it should be limited and the associated risks weighted against the benefits.

Protocols: 1. For a selection of users with dial-up access, review authorization and justification.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.8.6 Owners periodically review access authorization listings and determine whether they remain appropriate.

References:
FISCAM: TAC-2.1.2

Related CSRs: 1.4.1, 2.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The owner should identify the nature and extent of access to each resource that is available to each user. A good approach is to build an architecture matrix of personal and data access functions.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.1 If a CMS Business Partner is part of a larger organization, the Business Partner must implement policies and procedures that protect CMS sensitive information from unauthorized access by the larger organization.

References:
HIPAA: 164.308(a)(4)(ii)(A)

Related CSRs: 1.4.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review security policies and procedures for business partner access.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Interview a sample of users to confirm the required understanding and access authorizations.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.2 Public users (i.e., users who have not been authenticated) only have access to the extent necessary to accomplish mission objectives while preventing unauthorized access to sensitive information. The user actions that can be performed by public users on the information system have been identified and documented.

References:
ARS: AC-14.0
ARS: AC-14.1
NIST 800-53: AC-14
PISP: 4.3.2.14

Related CSRs: 2.10.5, 3.2.3, 10.7.8, 10.8.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that identify which specific user actions can be performed without I&A.

Protocols: 1. Examine organizational records or documents to determine what specific user actions can be performed on the information system without requiring identification and authentication.
2. Examine the configuration settings of the information system to determine if the system allows users to perform certain actions on the system without identifying and authenticating to the system in accordance with access control policy and procedures.
3. Test the information system by attempting to perform actions that are permitted without identification and authorization to determine if those actions can be performed in accordance with access control policy and procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the permitted actions without identification and authentication control is implemented.
5. Test the information system by attempting to perform actions that are not permitted for a user that has not been identified or authenticated to the information system (e.g., administrator functions).
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently identifies actions permitted on the information system without requiring user identification or authentication on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the permitted actions without identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the organization limits specific user actions that can be performed without identification and authentication to only the actions required to accomplish mission objectives.
9. Examine the configuration settings of the information system to determine if the system allows users to perform certain mission related actions without identifying and authenticating to the system.
10. Test the information system by attempting to perform actions that are not defined by the access control policy and procedures as being the minimum actions necessary to accomplish mission objectives without identification and authentication, to determine if the access controls are working as intended.

2.9.3 User identification is required for any transaction that has information security implications.

References:
ARS: IA-2.CMS-1
ARS: IA-CMS-1.CMS-1
NIST 800-53: IA-2
PISP: 4.3.1.1
PISP: 4.3.1.2

Related CSRs: 2.2.3, 7.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Help desk policy should require individual identification before transactions can be completed.

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system uniquely identifies users and if authentication of user identities is accomplished through the use of passwords, tokens, or biometrics.
2. Examine organizational records or documents and the information system configuration settings to determine if passwords, tokens, or biometrics meet Level 1, 2, 3, or 4 requirements consistent with NIST SP 800-63.
3. Test the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST SP 800-63.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user identification and authentication control is implemented.
5. Examine organizational records or documents to determine if identification and authentication mechanisms are employed at the application level.
6. Test the appropriate components within the information system to determine if passwords, tokens, or biometrics meet Level 3 or 4 requirements consistent with NIST SP 800-63.
7. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently identifies and authenticates users on an ongoing basis.
8. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine organizational records or documents and the information system configuration settings to determine if multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics.
10. Test the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ multifactor authentication.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.4 The use of passwords and access control measures are in place to identify who accessed protected information, limit that access to persons with a need-to-know, and prohibit the use of access scripts containing embedded passwords.

References:
FISCAM: TAC-3.2.A
HIPAA: 164.312(a)(1)
HIPAA: 164.312(e)(1)

Related CSRs: 2.2.3, 2.5.4, 2.7.2, 7.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Logical access controls should be designed to restrict legitimate users to the specific system(s), programs, and files they need and prevent others, such as hackers, from entering the system at all.

Protocols: 1. Inspect a sample of access audit data supporting continuing use to the required process.
2. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing.
3. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description.
4. Review documentation describing audit systems implemented to record all accesses, including access scripts, to protected information.
5. Review Access Authorization Lists to confirm designation of all users allowed access to each separate security partition within the system (e.g. each platform root logon, each application relating to a unique separation of duties boundary, and each network device that supports direct logon).
6. Review relevant policies and procedures for inclusion and directed use of the required process.

2.9.5 Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.

References:
HIPAA: 164.308(a)(4)(ii)(B)

Related CSRs: 2.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The mechanisms are used to authenticate users before granting them access permissions to the system or application.

Protocols: 1. Review documentation establishing that authorization control exists, and includes the required feature.

2.9.6 Users maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others, and report lost items immediately.

References:
FISCAM: TAC-3.2.A.8

Related CSRs: 1.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Factors that affect the use of these devices include (1) the frequency that possession by authorized users is checked, and (2) users' understanding that they should not allow others to use their identification devices.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Interview a sample of users to confirm the required understanding and device possession.

2.9.7 Passwords are distributed securely and users are informed not to reveal their passwords to anyone (e.g., social engineering). A process is in place for handling lost and compromised passwords.

References:
ARS: IA-5.0
NIST 800-53: IA-5
PISP: 4.3.1.5

Related CSRs: 1.1.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Users take reasonable measures to safeguard passwords, including not loaning or sharing passwords with others, and reporting lost or compromised passwords immediately.

Protocols: 1. Examine organizational records or documents to determine if the organization establishes administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
2. Interview selected organizational personnel with identification and authentication responsibilities to determine if users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator management control is implemented.
4. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently manages authenticators for the information system on an ongoing basis.
5. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator management control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: *Access Control*

General Requirement

Control Technique

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.8 Entity authentication (the corroboration that an entity is the one claimed) exists and includes a unique user identifier and automatic logoff after a predetermined amount of time (normally 15 minutes). It also requires multifactor authentication (password combined with token, password with biometric, etc.) that is NIST SP 800-63 level 4 compliant for remote system access.

Related CSRs: 10.8.2, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: IA-2.1
ARS: IA-2.CMS-1
HIPAA: 164.312(a)(2)(i)
HIPAA: 164.312(a)(2)(iii)
HIPAA: 164.312(d)
NIST 800-53: IA-2
NIST 800-53: IA-4
PISP: 4.3.1.2

Guidance: Procedures should be in place to authenticate users before granting them access to the system or application.

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system uniquely identifies users and if authentication of user identities is accomplished through the use of passwords, tokens, or biometrics.
2. Examine organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers.
3. Examine organizational records or documents and the information system configuration settings to determine if remote user passwords, tokens, or biometrics meet Level 4 requirements consistent with NIST SP 800-63.
4. Examine organizational records or documents to determine if a personal identity card or token is used to uniquely identify and authenticate employees and contractors.
5. Test the information system to determine if remote user passwords, tokens, or biometrics meet Level 4 requirements consistent with NIST SP 800-63.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user identification and authentication, and identifier management controls are implemented.
7. Examine organizational records or documents to determine if identification and authentication mechanisms are employed at the application level.
8. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently identifies and authenticates users on an ongoing basis.
9. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently manages user identifiers for the information system on an ongoing basis.
10. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user identification and authentication, and identifier management controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Examine organizational records or documents and the information system configuration settings to determine if remote access multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics.
12. Test the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ remote access multifactor authentication.

Category: *Access Control*

General Requirement

Control Technique

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.9 For password-based authentication, passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) not displayed when entered; (4) changed every 60 days, when an individual changes positions, or when security is breached; (5) at least 8 characters in length; (6) must include at least one number, one upper and lower case character, and one special character; (7) prohibited from reuse for at least 6 generations; (8) prohibited from being changed more than once in a 24-hour period; and (9) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.

Related CSRs: 1.1.1, 3.6.2, 7.3.3, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: IA-2.CMS-2
ARS: IA-4.0
ARS: IA-5.0
ARS: IA-6.0
CMS: Directed
FISCAM: TAC-3.2.A.1
FISCAM: TAC-3.2.A.2
FISCAM: TAC-3.2.A.4
HIPAA: 164.308(a)(5)(ii)(D)
NIST 800-53: IA-2
NIST 800-53: IA-4
NIST 800-53: IA-5
NIST 800-53: IA-6
PISP: 4.3.1.2
PISP: 4.3.1.4
PISP: 4.3.1.5
PISP: 4.3.1.6

Guidance: Policies and procedures should exist that implement these minimum password requirements. The use of alphanumeric passwords reduces the risk that an unauthorized user could gain access to a system by using a computer to try dictionary words or names until the password is guessed.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers.
2. Examine organizational records or documents and the information system configuration settings to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.
3. Examine organizational records or documents and the information system configuration settings to determine if passwords, tokens, or biometrics meet Level 1, 2, 3, or 4 requirements consistent with NIST SP 800-63.
4. Test the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST SP 800-63.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identifier management control is implemented.
6. Examine organizational records or documents to determine if the organization establishes administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
7. Examine organizational records or documents and information system configuration settings to determine if the system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).
8. Test the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism.
9. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator feedback control is implemented.
10. Interview selected organizational personnel with identification and authentication responsibilities to determine if users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.
11. Examine organizational records or documents to determine if the information system establishes user control of the corresponding private key and maps the authenticated identity to the user account (for PKI-based authentication).
12. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently identifies and authenticates users on an ongoing basis.
13. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.
14. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently obscures feedback of authentication information during the authentication process on an ongoing basis.
15. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently manages user identifiers for the information system on an ongoing basis.
16. Test the information system to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.
17. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the identifier and authenticator management control are documented and the resulting information used to actively improve the control on a continuous basis.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

18. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator management control are documented and the resulting information used to actively improve the control on a continuous basis.
19. Examine organizational records or documents and the information system configuration settings to determine if multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics.
20. Test the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ multifactor authentication.

2.9.10 Systems are configured to disable access for 15 minutes after 3 failed logon attempts. User account lockout results from 3 consecutive disable cycles, and requires an administrator-level reset to restore access to the user account.

References:
ARS: AC-7.0
FISCAM: TAC-3.2.A.5
NIST 800-53: AC-7
PISP: 4.3.2.7

Related CSRs: 2.6.1, 7.3.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Procedures should exist for resetting logon features after three failed attempts. To prevent guessing of passwords, attempts to log onto the system with invalid passwords should be limited.

Protocols: 1. Examine organizational records or documents to determine if the information system in accordance with access control policy and procedures: (i) enforces the maximum number of consecutive invalid access attempts within a certain period of time; (ii) automatically enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period; and (iii) enforces automatic locks on the account/node for an organization-defined time period or delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
2. Examine the information system configuration settings to determine if the information system enforces organizational policy and procedures for unsuccessful login attempts.
3. Test the account lockout policy on selected user accounts by exceeding the maximum number of invalid login attempts within the organization-defined time period on the information system to determine if the information system locks the account/node.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the unsuccessful login attempts control is implemented.
5. Test the account lockout policy on selected accounts by establishing initial lockout by exceeding the maximum number of invalid logon attempts, and then attempt to: (i) login to the account in less than the organization-defined delay lockout time period; and (ii) login to the account after the organization-defined lockout period to determine if the information system lockout/delay policy is being enforced.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces limitations on consecutive invalid access attempts on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the unsuccessful login attempts control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine the information system configuration settings to determine if the information system is configured to automatically lock the account/nodes until released by the administrator when the maximum number of unsuccessful attempts is exceeded.
9. Test the account lockout mechanism by locking out selected accounts when exceeding the maximum number of invalid logon attempts, and then attempting to login to the accounts both before the administrator releases the locked accounts and after the administrator releases the locked accounts to determine if the information system administrator account lock release operates as intended.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.11 When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) authentication is provided through UserID and password encryption for use over public telephone lines; (2) standard access is provided through a toll-free number and through local telephone numbers to local data facilities; and (3) both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards should have both identification and authentication features and provide for data encryption.

References:
FISCAM: TAC-3.2.E.1
IRS 1075: 5.8@5.1
IRS 1075: 5.8@5.2
IRS 1075: 5.8@5.2.a
IRS 1075: 5.8@5.2.c
IRS 1075: 5.8@5.2.d

Related CSRs: 3.6.1, 3.6.3, 10.8.2, 10.10.3, 10.10.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The entity should have cost-effective physical and logical controls in place for protecting systems accessed remotely. The purpose of this CSR is to prevent unauthorized access or disclosure of PHI by implementing controls that reflect industry security standards. Without authentication, the system cannot verify the provider or supplier is who they claim to be. Without encryption, the system cannot protect the data while in transit. If the PHI is under the control of the business partner, it is expected they will provide reasonable protection. Where the business partner considers the cost is excessive, they should seek alternative controls that will be more cost effective. For example; if modems are already implemented without encryption, the business partner may propose software encryption as an alternate control. In the event the business partner is unable to find less expensive alternatives, they need to provide a cost to meet this CSR in a Safeguard. CMS will then consider the cost and associated risk in funding these solutions over time.

Protocols: 1. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.
2. Review audit data, including spot inspections, confirming that all the specified controls are applied to all dialup access. This includes review of all devices having potential access to sensitive information that are equipped with modems.
3. Review documentation describing implementation of the specified controls for all dialup access to systems handling sensitive information. (Controls for packet switched network access are covered in other control techniques.)
4. Review relevant policies and procedures for inclusion and directed use of the required process.

2.9.12 In any local or remote session, inactivity at any workstation during any 15 minute period causes the system to automatically terminate (disable) workstation access to the system. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords are utilized where supported by existing operating systems.

References:
ARS: AC-11.0
ARS: AC-12.0
ARS: SC-10.0
ARS: SC-10.CMS-1
ARS: SC-10.CMS-2
CMS: Directed
FISCAM: TAC-3.2.C.3
HIPAA: 164.310(b)
NIST 800-53: AC-11
NIST 800-53: AC-12
NIST 800-53: SC-10
PISP: 4.3.2.11
PISP: 4.3.2.12
PISP: 4.3.4.10

Related CSRs: 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Workstation and desktop time-outs and password protected screen savers are important access controls used to prevent unauthorized users from accessing the system using the logged-on users credentials.

Protocols: 1. Examine the configuration settings of the information system to determine if the system automatically terminates a session after the organization-defined time period of inactivity.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the session termination control is implemented.
3. Examine the configuration settings of the information system to determine if the system initiates a session lock until the user reestablishes access using appropriate identification and authentication procedures.
4. Test the session lock mechanism by allowing a user session to remain inactive for the organization-defined period to determine if the session lock automatically occurs on the information system and that the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently employs a session lock capability on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the session lock control are documented and the resulting information used to actively improve the control on a continuous basis.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.13 The number of concurrent sessions is limited and enforced to a single session for all users. The information system is configured to notify the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful log on attempts since the last successful logon.

References:
ARS: AC-10.0
ARS: AC-9.0
CMS: Directed
NIST 800-53: AC-10
NIST 800-53: AC-9
PISP: 4.3.2.10
PISP: 4.3.2.9

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establishing and enforcing concurrent session limits assists in preventing users from having unnecessary sessions open.

Protocols: 1. Examine the configuration settings of the information system to determine if upon successful logon, the system displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.
2. Examine the configuration settings of the information system to determine if the system limits the number of concurrent sessions for users to an organization-defined number of sessions.
3. Test the information system by viewing a selection of user logons to the system to determine if upon successful logon, the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon are displayed.
4. Test the concurrent session control by attempting to exceed the organization-defined number of concurrent sessions with a valid user account.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the previous logon notification and concurrent session controls are implemented.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently limits the number of concurrent sessions and provides users with essential logon information on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the previous logon notification control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the concurrent session control are documented and the resulting information used to actively improve the control on a continuous basis.

2.9.14 The information system obscures feedback of authentication information (e.g., displaying asterisks when a user types in a password or token authentication code) during the authentication process to protect the information from possible exploitation by unauthorized individuals.

References:
ARS: IA-6.0
NIST 800-53: IA-6
PISP: 4.3.1.6

Related CSRs: 10.2.10

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Keeping the system authentication feedback information confidential prevents the authentication mechanisms from being revealed to outside users.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).
2. Test the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator feedback control is implemented.
4. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently obscures feedback of authentication information during the authentication process on an ongoing basis.
5. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator feedback control are documented and the resulting information used to actively improve the control on a continuous basis.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.15 System administrators maintain separate user accounts with separate UserIDs and passwords; one exclusively for standard user functions (e.g., Internet, e-mail, etc.) and one for system administration activities. These UserIDs are not shared with anyone.

References:
ARS: IA-2.CMS-1
ARS: IA-4.CMS-1
NIST 800-53: IA-2
NIST 800-53: IA-4
PISP: 4.3.1.2
PISP: 4.3.1.4

Related CSRs: 2.1.3, 2.1.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Available procedures define the usage of the unique UserIDs.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers.
2. Examine organizational records or documents to determine if a personal identity card or token is used to uniquely identify and authenticate employees and contractors.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user identification and authentication, and identifier management controls are implemented.
4. Examine organizational records or documents to determine if identification and authentication mechanisms are employed at the application level.
5. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization manages user identifiers for the information system, and the information system consistently identifies and authenticates users on an ongoing basis.
6. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the identifier management, and user identification and authentication controls are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents and the information system configuration settings to determine if multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics.
8. Test the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ multifactor authentication.

2.9.16 Unique and separate administrator accounts based on the users' roles and responsibilities are used for administrator versus non-administrator activities. Where multiple administrators are employed, maintain a limited number who have full access. Centralized control of user access administrator functions is implemented.

References:
ARS: AC-2.CMS-2
ARS: AC-2.CMS-3
ARS: AC-5.CMS-2
NIST 800-53: AC-2
NIST 800-53: AC-5
PISP: 4.3.2.2
PISP: 4.3.2.5

Related CSRs: 2.1.3, 2.1.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The use of unique and separate accounts helps to ensure that administrative activities are kept separate from non-administrative activities.

Protocols: 1. Examine organizational records or documents to determine if the information system enforces separation of duties.
2. Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
5. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
6. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
7. Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.
8. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.
9. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
11. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.17 Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system. Information system accounts are reviewed every 30 days.

References:
ARS: AC-2.1
FISCAM: TAC-3.2.A.6
NIST 800-53: AC-2
PISP: 4.3.2.2

Related CSRs: 1.10.3, 1.10.4, 2.2.18

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist for terminating system access for all users no longer requiring access. This does not have to be an automated process but any process that is automatically followed when a user is terminated or transferred.

Protocols:
1. Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
2. Examine organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures.
3. Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation.
4. Examine a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled.
5. Examine a list of recently separated or terminated employees to determine if the organization removed accounts for these individuals according to established procedures and completed any organization-required documentation.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.
10. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.
11. Examine organizational records or documents to determine if temporary and emergency accounts are automatically terminated after the organization-defined time period for each type of account.
12. Examine the information system configuration settings to determine if the settings are set to automatically terminate temporary and emergency accounts after the organization-defined time period.
13. Examine organizational records or documents to determine if any temporary or emergency accounts have not been terminated after the organization-defined time period.
14. Test the information system to determine if temporary and emergency accounts are automatically terminated after exceeding a set time period.
15. Examine organizational records or documents to determine if inactive accounts on the information system are automatically disabled after the organization-defined time period.
16. Examine the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after the organization-defined time period.
17. Examine organizational records or documents to determine if any inactive accounts on the information system have not been disabled after the organization-defined time period, (i.e., if the last login date exceeds the organization-defined time period for disabling inactive accounts).
18. Test the information system to determine if inactive accounts are automatically disabled after exceeding the organization-defined time period.
19. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and that appropriate individuals are notified of these occurrences.
20. Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.18 Inactive user accounts are monitored and automatically disabled when not needed or after 30 days of inactivity, and disabled accounts are removed during the annual recertification process.

References:
ARS: AC-2.3
ARS: IA-4.0
FISCAM: TAC-3.2.C.4
NIST 800-53: AC-2
NIST 800-53: IA-4
PISP: 4.3.1.4
PISP: 4.3.2.2

Related CSRs: 1.10.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Inactive accounts should be monitored and revoked when no longer required.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers.
2. Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
3. Examine organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures.
4. Examine a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled.
5. Examine a list of recently separated or terminated employees to determine if the organization removed accounts for these individuals according to established procedures and completed any organization-required documentation.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.
9. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.
10. Examine organizational records or documents to determine if inactive accounts on the information system are automatically disabled after the organization-defined time period.
11. Examine the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after the organization-defined time period.
12. Examine organizational records or documents to determine if any inactive accounts on the information system have not been disabled after the organization-defined time period, (i.e., if the last login date exceeds the organization-defined time period for disabling inactive accounts).
13. Test the information system to determine if inactive accounts are automatically disabled after exceeding the organization-defined time period.
14. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and that appropriate individuals are notified of these occurrences.
15. Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.

2.9.19 Vendor-supplied passwords are replaced immediately.

References:
FISCAM: TAC-3.2.A.3

Related CSRs: 3.6.2, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Vendor supplied passwords are known by every hacker and they are usually the first passwords tried by hackers.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. For a sample of applications and network devices, attempt to log on using common vendor-supplied passwords. These default passwords are usually documented in the associated manuals.

Category: *Access Control*

General Requirement

Control Technique

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.20 A callback capability with re-authentication is used to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a UserID and password, and enters the network through the standard authentication process. Access to such systems is authorized and recorded. UserIDs assigned to vendors are recertified annually.

References:

ARS: AC-17.CMS-3
NIST 800-53: AC-17
PISP: 4.3.2.17

Related CSRs: 3.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that specify the callback measures

Protocols: 1. Examine organizational records or documents to determine if remote access is: (i) monitored on aperiodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs.
2. Examine organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures.
3. Examine organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials.
4. Examine the configuration of the information system to determine if controls are employed to restrict remote access to the system.
5. Examine a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented.
7. Test the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs remote access controls for the information system on an ongoing basis.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Examine organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods.
11. Examine organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures.
12. Test the automated mechanism(s) within the information system to determine if each of the functions associated with the monitoring and control of remote access produce accurate and informative information, in accordance with remote access monitoring policy and procedures.
13. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.
14. Examine a remote access connection to the information system to determine if the connection requires the use of encryption and encryption is actually employed.
15. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization controls remote access through a managed access control point.
16. Test remote access controls by attempting to connect remotely to the information system without connecting through the managed access control point to determine if remote access can be achieved without following organizational policy and procedures.

Category: ***Access Control***

General Requirement

Control Technique

2.10 Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure.

2.10.1 Security software is used to restrict access. Only explicitly authorized information security personnel have access to system security functions deployed in hardware, software, and firmware.

References:
ARS: AC-3.1
FISCAM: TAC-3.2.C.1
FISCAM: TAC-3.2.C.2
NIST 800-53: AC-3
PISP: 4.3.2.3

Related CSRs: 2.5.9, 3.6.4, 3.6.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The most commonly used means of restricting access to data files and software programs is through the use of access control software, also referred to as security software. Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted.

Protocols: 1. Examine organizational records or documents to determine if user access to the information system is authorized.
2. Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy.
3. Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling access to the system on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization explicitly defines security functions for the information system.
8. Examine organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy.
9. Test selected accounts that have access to information system security functions to determine if the user privileges for those accounts function as documented in accordance with authorization requirements.

2.10.2 Security administration personnel set parameters in security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files and operating system files. Standardized naming conventions are used for resources.

References:
FISCAM: TAC-3.2.C.5
FISCAM: TAC-3.2.C.6

Related CSRs: 2.1.6, 3.6.5, 6.4.1, 6.4.2, 6.8.1, 7.1.2, 7.2.1

Applicability: COB, CWF, DC, EDC, PSC

Guidance: The most commonly used means of restricting access to data files and software programs is through the use of access control software. Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Generally, access control software provides many access control options that must be activated and tailored to the entity's needs in order to be effective.

Protocols: 1. Review documentation describing the standardized naming conventions in use for resources.
2. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.
3. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
4. Perform penetration testing by attempting to access and browse computer resources.
5. Review relevant policies and procedures for inclusion and directed use of the required process.

2.10.3 Modification of data is restricted to authorized employees.

References:
CMS: Directed

Related CSRs: 7.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Logical access controls provide a technical means of controlling what information users can access (in accordance with relevant policy), the programs they can run, and the modifications they can make. Logical access controls may be implemented internally to the computer system being protected or may be implemented in external devices.

Protocols: 1. Review documentation of the control used to restrict of data updating to authorized employees.
2. Inspect a sample of audit data confirming that the required process is consistently used.
3. Inspect the Access Authorization List(s) identifying employees who are authorized to update data.
4. Review relevant policies and procedures for inclusion and directed use of the required process.

2.10 Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure.

2.10.4 Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, uncatalog, scratch, and rename a file.

References:
CMS: Directed

Related CSRs: 7.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Utilities for file access and related processing need controls in place.

Protocols: 1. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation of the process used to provide the specified control over routines that modify the status of a file.

2.10.5 Operating system controls are configured to disable public “read” and “write” access to all system files, objects, and directories. Operating system controls are configured to disable public “read” access to files, objects, and directories that contain sensitive information.

References:
ARS: AC-3.1
ARS: AC-3.CMS-4
ARS: AC-6.CMS-5
ARS: SC-14.CMS-1
NIST 800-53: AC-3
NIST 800-53: AC-6
NIST 800-53: SC-14
PISP: 4.3.2.3
PISP: 4.3.2.6
PISP: 4.3.4.14

Related CSRs: 1.9.3, 2.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that the OS controls are implemented to disable public read and write access to sensitive information.

Protocols: 1. Examine organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
2. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if, for publicly available information systems, the system protects the integrity of the information and applications and how the protections are implemented.
3. Examine organizational records or documents to determine what access rights/privileges the organization assigns to user tasks.
4. Examine selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks.
5. Test the publicly available information system by attempting to alter protected information using a public account to determine if access is limited in order to preserve the integrity of the information and the applications.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the public access protections control is implemented.
8. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently protects the integrity of the information and applications on public access systems on an ongoing basis.
9. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the public access protections control are documented and the resulting information used to actively improve the control on a continuous basis.

2.11 Logical controls shall be implemented for databases and DBMS software.

2.11.1 Access and changes to DBMS software are controlled. Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.

References:
FISCAM: TAC-3.2.D.3
FISCAM: TAC-3.2.D.4
HIPAA: 164.310(a)(2)(iii)

Related CSRs: 3.4.1, 6.5.1, 6.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. In addition, DBMS software changes should be protected from unauthorized changes through the use of logical access controls.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review the controls protecting DBMS software.

2.11 Logical controls shall be implemented for databases and DBMS software.

2.11.2 The use of database management system (DBMS) utilities is limited. DBMS and data dictionary controls have been implemented that: (1) restrict access to data files at the logical data view, field and field-value level; (2) implement column-level access controls; (3) control access to the data dictionary using security profiles and passwords; (4) maintain audit records that allow monitoring of changes to the data dictionary; and (5) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.

References:
ARS: AC-3.CMS-3
ARS: AC-6.CMS-4
FISCAM: TAC-3.2.D.2
NIST 800-53: AC-3
NIST 800-53: AC-6
PISP: 4.3.2.3
PISP: 4.3.2.6

Related CSRs: 2.1.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. In addition, use of DBMS utilities should be protected through the use of logical access controls and audit records.

Protocols: 1. Examine organizational records or documents to determine if user access to the information system is authorized.
2. Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy.
3. Examine organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
4. Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.
5. Examine organizational records or documents to determine what access rights/privileges the organization assigns to user tasks.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented.
7. Examine selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks.
8. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces the most restrictive set of rights/privileges or accesses needed by users on an ongoing basis.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least privilege control are documented and the resulting information used to actively improve the control on a continuous basis.

2.12 Sensitive material shall be protected.

2.12.1 Access to sensitive information is limited to those who are authorized by law or regulation. Physical and systemic barriers are reviewed/reported. Assessments are conducted of facility security features.

References:
ARS: PE-3.CMS-1
IRS 1075: 6.3@5
NIST 800-53: PE-3
PISP: 4.2.2.3

Related CSRs: 1.12.6, 2.5.4, 2.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Physical security controls augment technical means for controlling access to information and processing. It is important to review the effectiveness of physical access controls, both during normal business hours and at other times - particularly when an area may be unoccupied. Effectiveness depends on both the characteristics of the control devices used (e.g., keycard-controlled doors) and the implementation and operation.

Protocols: 1. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
2. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
3. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls physical access to the facility where the information system resides on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access control are documented and the resulting information used to actively improve the control on a continuous basis.

2.12 Sensitive material shall be protected.

2.12.2 Medicare data is not released to outside personnel unless the personnel are authorized to receive the data and their identity is verified.

References:
CMS: Directed

Related CSRs: 1.3.2, 1.3.7, 10.3.1, 10.3.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be procedures used to verify that outside personnel who request Medicare data are authorized to receive the data before releasing it.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.13 Suspicious access activity shall be investigated and appropriate action taken.

2.13.1 SSOs investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken and violations are summarized and reported to senior management.

References:
FISCAM: TAC-4.3.1
FISCAM: TAC-4.3.2
FISCAM: TAC-4.3.3

Related CSRs: 3.1.1, 7.1.1, 7.2.2, 7.3.4, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations should be investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur, repair any damage. The seriousness of the issue should determine what disciplinary actions might be taken. A good approach is to tie these violations/accidents into performance evaluations.
The frequency and magnitude of security violations and corrective actions taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the entity's operations, and any need for additional controls.

Protocols: 1. Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
2. Interview senior management and personnel responsible for summarizing violations.
3. Inspect audit data confirming that the required process is consistently used.

2.13.2 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.

References:
FISCAM: TAC-4.3.4

Related CSRs: 3.1.1, 3.1.2, 3.4.1, 7.3.4, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Once it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur and repair any damage that has been done.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.13.3 Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.

References:
CMS: Directed
IRS 1075: 3.2@2.4

Related CSRs: 2.2.13, 2.8.3, 6.4.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The process of inventorying and documenting missing tapes containing sensitive information should be integrated into the normal business processes of the organization.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.14 Owners shall determine disposition and sharing of data.

2.14.1 Standard forms are used to document approval for archiving, deleting, and sharing data files.

References:
FISCAM: TAC-2.3.1

Related CSRs: 1.3.7, 2.8.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard forms should be used and maintained on file to document the users' approvals.

Protocols: 1. Inspect standard approval forms.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

2.14 Owners shall determine disposition and sharing of data.

2.14.2 Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

References:
FISCAM: TAC-2.3.2
HSPD-7: H(25)(b)

Related CSRs: 1.11.3, 1.11.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Resource owners should determine if, with whom, and by what means information resources can be shared. When files are shared with other entities, it is important that (1) data owners understand the related risks and approve such sharing, and (2) receiving entities understand the sensitivity of the data involved and safeguard the data accordingly. This should normally require a written agreement prior to the sharing of sensitive information.

Protocols: 1. Examine documents authorizing file sharing and file sharing agreements.

3. System Software

3.1 Inappropriate or unusual activity shall be investigated and appropriate actions taken.

3.1.1 Measures define investigation of inappropriate or unusual activity and the appropriate actions to be taken.

References:
ARS: AU-6.CMS-3
FISCAM: TSS-2.2.2
NIST 800-53: AU-6
PISP: 4.3.3.6

Related CSRs: 2.6.1, 2.8.4, 2.13.1, 2.13.2, 4.2.2, 8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The possibility of damage or alteration to the system software, application software, and related data files should be investigated and needed corrective actions taken. For example, policy guideline actions should include notifying the resource owner of the violation.

Protocols: 1. Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
2. Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.
4. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
7. Test the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities by artificially generating auditable events and monitoring the results.
8. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.
9. Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.

Category: ***System Software***

General Requirement

Control Technique

3.1 Inappropriate or unusual activity shall be investigated and appropriate actions taken.

3.1.2 Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).

References:
ARS: CA-7.CMS-1
FISCAM: TSS-2.2.4
NIST 800-53: CA-7
PISP: 4.1.4.7

Related CSRs: 1.2.3, 1.5.4, 1.8.1, 1.8.2, 1.8.3, 1.8.5, 1.8.8, 2.13.2, 4.4.1, 6.3.14

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to include the evaluation of the software control techniques in the risk assessment with annual reviews. If there are any suspicious functions or processes occurring then the suspicious event should be investigated immediately.

Protocols: 1. Examine organizational records or documents to determine if the organization monitors the security controls in the information system on an ongoing basis.
2. Examine organizational records or documents to determine if the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.
3. Examine organizational records or documents to determine if the organization: (i) assesses designated security controls in the information system; (ii) analyzes for impact, documents, and reports changes to or deficiencies in the operation of the security controls; and (iii) makes adjustments to the information SSP and POA&M, as appropriate.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the continuous monitoring control is implemented.
5. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently monitors the security controls in the information system on an ongoing basis.
6. Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the continuous monitoring control are documented and the resulting information used to actively improve the control on a continuous basis.

3.1.3 The use of privileged system software and utilities is reviewed by technical management.

References:
FISCAM: TSS-2.2.1

Related CSRs: 1.8.2, 3.3.3, 4.1.1, 4.3.1, 4.6.1, 10.7.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Privileged access may be used only to perform assigned job duties.

Protocols: 1. Some good questions to ask about privileged system software and utilities are: - Are the system privileges granted to users strictly on need to use basis? - Are there separate UserIDs for performing privileged and normal activities? - Are the log in privileges for highly privileged accounts available only from console and terminals situated within the console room? - Is the audit record maintained of activities conducted by highly privileged users? - How long is it preserved?
2. Review documentation for system software utilities and verify that technical management has given use approvals.
3. Review documentation supporting technical management reviews.
4. Interview technical management regarding their reviews of privileged system software and utilities usage.

3.1.4 Systems programmers' activities are monitored and reviewed.

References:
FISCAM: TSS-2.2.3

Related CSRs: 3.2.2, 4.2.2, 4.4.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: System programmers and/or system administrators need supervisor rights to make modifications. These personnel need additional controls in place to prevent misuse of these rights. All programmers need monitoring. The monitoring controls which are set globally for all programmers include: displaying sign-on information to the user which indicates the date and time of their last sign-on and any unauthorized sign-on attempts; monitoring the number of minutes of terminal inactivity before either canceling a job or disconnecting from a terminal; setting a limit to a user's ability to log on to multiple terminals with the same UserID at the same time; the ability to distinguish between local and remote sign on in order to prevent remote accesses completely or require normal logon security for remote access; and supervisors and managers review the activities process.

Protocols: 1. System Programmer and/or System Administrators need supervisor rights to make modifications. These personnel need additional controls in place to prevent misuse of these rights.
2. Review documentation supporting the supervising and monitoring of systems programmers' activities.
3. Determine that system programmer supervisors are supervising and monitoring their staff.

3.1.5 Systems support alarm features to provide immediate notification of predefined events.

References:
HIPAA: 164.312(b)

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 2.1.13, 4.1.1, 4.1.4, 9.3.1, 9.3.5, 9.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is a good practice to have an automated audit system perform the immediate notification.

Protocols: 1. Review audit records.
2. Review security plan to determine use of audit records and alarms set points.

Category: ***System Software***

General Requirement

Control Technique

3.2 Policies and techniques shall be implemented for using and monitoring system utilities.

3.2.1 Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.

References:
FISCAM: TSS-2.1.2

Related CSRs: 1.1.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security training is adjusted to the level of the system programmer's responsibilities. The FISCAM defines a system programmer as someone who develops and maintains system software and related utilities.

Protocols: 1. Interview systems programmers regarding their responsibilities.
2. Verify that the appropriate responsibilities have been defined.

3.2.2 Responsibilities for monitoring use are defined and understood by technical management. Procedures for using and monitoring use of system software utilities are implemented and are up-to-date.

References:
FISCAM: TSS-2.1.1
FISCAM: TSS-2.1.3

Related CSRs: 1.1.3, 1.4.8, 3.1.4, 4.1.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security training is adjusted to the level of the technical management's responsibilities. It is a good practice to identify access for various programs and utilities, monitoring, and written policies and procedures. As part of the System Security Plan, policies and procedures for using and monitoring the use of system software utilities should be defined and documented.

Protocols: 1. Interview technical management regarding their responsibilities.
2. Verify that the appropriate responsibilities are defined.
3. Interview management and systems personnel.
4. Verify the existence and current version of the appropriate policies and procedures.

3.2.3 Privilege restrictions are enabled to limit public and employee access to administrator tools, scripts, and utilities. The use of sensitive system tools, scripts, and utilities is recorded using access control software reports or job accounting data (e.g., IBM's System Management Facility).

References:
ARS: AC-3.CMS-3
FISCAM: TSS-2.1.4
NIST 800-53: AC-3
PISP: 4.3.2.3

Related CSRs: 1.9.2, 2.1.4, 2.9.2, 9.6.6, 10.7.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The output report record is a good management tool to assist in tracking the usage of sensitive system utilities. The policy and procedures for the sensitive system utilities are normally depicted in the system security plan.

Protocols: 1. Examine organizational records or documents to determine if user access to the information system is authorized.
2. Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy.
3. Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling access to the system on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization explicitly defines security functions for the information system.
8. Examine organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy.
9. Test selected accounts that have access to information system security functions to determine if the user privileges for those accounts function as documented in accordance with authorization requirements.

3.3 Access authorizations shall be appropriately limited.

3.3.1 Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.

References:
FISCAM: TSS-1.1.2

Related CSRs: 1.1.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses.

Protocols: 1. Attempt to access the operating system and other system software.
2. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access.
3. Interview management and system personnel regarding access restrictions.
4. Review pertinent policies and procedures.

Category: ***System Software***

General Requirement

Control Technique

3.3 Access authorizations shall be appropriately limited.

3.3.2 Procedures for restricting access to systems software are implemented and are up-to-date. Justification and management approval for access to systems software is documented and retained.

References:
FISCAM: TSS-1.1.1
FISCAM: TSS-1.1.3

Related CSRs: 1.9.2, 1.9.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access to system software is restricted to a few system programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly. The SSO normally maintains an approved Access Control Listing (ACL) for all systems that process or transmit sensitive data. The individual's supervisor provides justification and approval to the SSO. The ACL is part of the System Security Profile.

Protocols: 1. Review pertinent policies and procedures.
2. Attempt to access the operating system and other system software.
3. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access.
4. Interview management and systems personnel regarding access restrictions.
5. Interview system manager and security administrator.

3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.

References:
FISCAM: TSS-1.1.4

Related CSRs: 2.8.2, 3.1.3, 4.6.1, 4.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security skill needs are accurately identified and included in job descriptions. The duties from the job description should be compared to the SSO's security access list and the security audit records. If these functions do not match, then management should take corrective action(s). The review memo should be provided to the SSO for inclusion in the System Security Profile.

Protocols: 1. Determine the last time the access capabilities of system programmers were reviewed.

3.4 Installation of system software shall be documented and reviewed.

3.4.1 Installation of all system software is recorded to establish an audit trail/record and is reviewed by data center management.

References:
FISCAM: TSS-3.2.4

Related CSRs: 2.3.1, 2.11.1, 2.13.2, 4.7.5, 6.3.6, 6.3.12, 6.3.14, 6.5.1, 6.6.1, 6.7.2, 6.8.2, 9.7.1, 9.8.1, 9.8.2, 9.8.3, 10.7.2, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good process for monitoring and documenting migration of system software is in the change management process for the organization.

Protocols: 1. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.
2. Interview data center management about their role in reviewing system software installations.

3.4.2 Migration of tested-and-approved system software to production use is performed by an independent library control group.

References:
FISCAM: TSS-3.2.2

Related CSRs: 4.7.5, 6.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good process for monitoring and documenting the migration of system software is in the change management process for the organization.

Protocols: 1. Interview management, systems programmers, and library controls personnel, and determine who migrates approved system software to production libraries, and whether versions are removed from production libraries.

3.4.3 Vendor-supplied system software includes software documentation and is supported by the vendor.

References:
FISCAM: TSS-3.2.5

Related CSRs: 4.1.5, 5.8.1, 6.3.13

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to include vendor maintenance with the purchase of the software.

Protocols: 1. Interview system software personnel concerning a selection of system software and documentation, and determine the extent to which the operating version of the system software is currently supported by the vendor.

3.4 Installation of system software shall be documented and reviewed.

3.4.4 Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.

References:
FISCAM: TSS-3.2.1

Related CSRs: 5.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: If possible, a good approach to scheduling major installations of system software is during off hours. This creates minimal impact on operations and provides time to back out the installation if errors occur. Notification can be provided several days in advance via email.

Protocols: 1. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
2. Review recent installations and determine whether scheduling and advance notification did occur.
3. Interview management and systems programmers about scheduling and giving advance notices when system software is installed.

3.4.5 All system software is current and has current and complete documentation. Outdated versions of system software are removed from production libraries.

References:
FISCAM: TSS-3.2.3
FISCAM: TSS-3.2.6

Related CSRs: 1.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An automated version tracking system can assist with tracking the current version of software and the software's documentation. Outdated versions are kept in a library other than the production library. In order to prevent redundant execution of older versions, they should be deleted from production and moved elsewhere. Storage for outdated versions may be part of the Contingency Plan reconstitution efforts.

Protocols: 1. Interview management and system programmers about the currency of system software, and the currency and completeness of software documentation.
2. Review documentation and test whether recent changes are incorporated.
3. Review supporting documentation from a few system software migrations and the removal of outdated versions from production libraries.

3.5 System software changes shall be authorized, tested and approved before implementation.

3.5.1 New system components and system software versions or products and modifications to existing system software receive proper authorization, are supported by a change request document, are tested, and the test results are approved before implementation.

References:
FISCAM: TSS-3.1.3
FISCAM: TSS-3.1.4

Related CSRs: 4.7.5, 5.7.4, 6.6.1, 6.7.2, 10.7.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This should be documented and provided in the Change management process. Change management standards, proper controls, processes, and procedures will provide for appropriate testing prior to implementation. A preformatted change request process provides efficiency and assists in the accuracy of the change tracking processes.

Protocols: 1. Select some emergency changes to system components and software, and test whether the indicated procedures were used.
2. Review procedures used to control and approve emergency changes.
3. Select a few recent system component and software changes and review audit data confirming that the specified process was followed.
4. Determine the procedures used to test and approve system components and software prior to its implementation.
5. Determine what authorizations and documentation are required prior to initiating system software changes.
6. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.

3.5.2 Controls exist and are up-to-date for identifying, selecting, installing and modifying system software. Controls include a mission/business impact analysis, including the training required to implement the controls; an analysis of costs and benefits; and consideration of the impact on processing reliability and security.

References:
FISCAM: TSS-3.1.1
NIST 800-53: CM-4
PISP: 4.2.4.4

Related CSRs: 1.4.1, 1.8.2, 1.9.2, 4.1.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Usually, the change request will contain most of the selection, installation, modification, and cost information.

Protocols: 1. Examine organizational records or documents to determine if the organization monitors changes to the information system and identifies the types of changes monitored.
2. Examine organizational records or documents to determine if the organization performs security impact analyses to assess the effects of changes to the information system.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring configuration changes control is implemented.
4. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently monitors configuration changes to the information system on an ongoing basis.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring configuration changes control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***System Software***

General Requirement

Control Technique

3.5 System software changes shall be authorized, tested and approved before implementation.

3.5.3 Procedures are implemented for identifying and documenting system software problems. This includes: (1) using a record to log the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.

References:
FISCAM: TSS-3.1.2

Related CSRs: 1.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to automate the software problem tracking processes. Monthly tracking reviews will assist in controlling any issues.

Protocols: 1. Review the causes and frequency of any recurring system software problems, as recorded, and ascertain if the change control process should have prevented these problems.
2. Interview management and systems programmers.
3. Review procedures for identifying and documenting system software problems.

3.5.4 Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.

References:
CMS: Directed

Related CSRs: 4.7.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Checkpoints and restart capabilities on jobs will assist in meeting performance goals.

Protocols: 1. Verify the existence of checkpoint and restart capabilities.

3.5.5 Procedures are implemented for controlling emergency changes. These procedures include: (1) authorizing and documenting emergency changes as they occur, (2) reporting the changes for management review, and (3) review of the changes by an independent IT supervisor.

References:
FISCAM: TSS-3.1.5
NIST 800-53: CM-3
PISP: 4.2.4.3

Related CSRs: 1.9.2, 5.7.2, 6.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to include emergency procedures in the change management process as well as appropriate procedures in the Contingency Plan

Protocols: 1. Examine organizational records or documents to determine if the organization documents and controls changes to the information system.
2. Examine organizational records or documents to determine if appropriate organizational officials approve information system changes in accordance with organizational policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration change control is implemented.
4. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently documents and controls information system configuration changes on an ongoing basis.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration change control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the organization employs automated mechanisms to manage configuration changes to the information system
7. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.

3.6.1 All accesses to system software files are recorded by automated recording facilities.

References:
FISCAM: TSS-1.2.2

Related CSRs: 2.2.24, 2.9.11, 10.7.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This is part of the application and system access controls. Included could be an alerting process when an automated notification process can identify suspicious recording or file changes occur.

Protocols: 1. Review sample accesses to system software files to confirm automated recording facilities.

Category: ***System Software***

General Requirement

Control Technique

3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.

3.6.2 All vendor-supplied default logins, passwords, and security parameters have been removed, disabled or reinitialized to more secure settings.

References:
ARS: AC-2.CMS-1
FISCAM: TSS-1.2.3
NIST 800-53: AC-2
NIST 800-53: IA-5
PISP: 4.3.2.2

Related CSRs: 1.9.2, 2.9.9, 2.9.19, 2.9.20, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Disabling default passwords and logins, and changing default security settings to more secure settings should be part of enhancing security (hardening) process when new software or systems are installed.

Protocols: 1. Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
2. Examine organizational records or documents to determine if the organization changes default authenticators upon information system installation.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.
4. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.
7. Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.

3.6.3 Remote access to the system master console is restricted. Physical and logical controls provide security over all workstations that are set up as master consoles.

References:
FISCAM: TSS-1.2.4

Related CSRs: 1.9.2, 2.2.19, 2.9.11, 10.10.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Only authorized personnel should have access to the master console(s). If all the procedures in access control are followed and proper physical control is provided then the master consoles should be secure.

Protocols: 1. Test to determine if the master console can be accessed, or if other terminals can be used to mimic the master console and take control of the system.
2. Determine what terminals are set up as master consoles and what controls exist over them.

3.6.4 Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access is generally limited to primary and backup systems programmers.

References:
ARS: AC-5.CMS-2
FISCAM: TSS-1.2.2
HIPAA: 164.310(a)(2)(iii)
NIST 800-53: AC-5
PISP: 4.3.2.5

Related CSRs: 2.10.1, 4.6.1, 10.7.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security skill needs are accurately identified and included in job descriptions. After necessary personnel have been identified, then corresponding access control software must be matched and implemented.

Protocols: 1. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
2. Using security software reports, determine who has access to system software files, security software, and audit files. Reports should be generated by the auditor, or at least in the presence of the auditor.
3. Examine organizational records or documents to determine if the information system enforces separation of duties.
4. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
5. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.
7. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***System Software***

General Requirement

Control Technique

3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.

3.6.5 The operating system is configured to prevent circumvention of the security software and application controls.

References:
FISCAM: TSS-1.2.1

Related CSRs: 2.2.4, 2.6.2, 2.10.1, 2.10.2, 10.7.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: System hardening should be part of operating system installation. Once the system is hardened then the security should be baselined and periodically updated. Additionally, an Intrusion Detection System, when possible, should be implemented for real time monitoring. A Host Intrusion Detection System would assist in preventing circumvention of controls.

Protocols: 1. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.
2. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.

3.6.6 The operating system's operational status and restart integrity is protected during and after shutdowns.

References:
ARS: SI-6.0
CMS: Directed
NIST 800-53: SI-6
PISP: 4.2.6.6

Related CSRs: 5.2.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good practice is to have qualified personnel standing by when systems are taken offline and when shutdowns occur. The QA team could provide a standard list for restart.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system verifies the correct operation of security functions upon system startup and restart, and/or upon command by users with appropriate privileges.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system notifies the system administrator, shuts the system down, or restarts the system when anomalies are discovered.
3. Examine the system configuration to determine if it verifies the correct operations of security functions upon system startup and restart, upon command by user with appropriate privilege, periodically and notifies system administrator, shuts the system down, restarts the system when anomalies are discovered.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security functionality verification control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently verifies the security functionality within the system on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to provide notification of failed security tests to appropriate personnel.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to support management of distributed security testing.

3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.

3.6.7 Secure information system recovery and reconstitution includes, but is not limited to: (1) resetting all system parameters (either default or organization-established), (2) reinstalling patches, (3) reestablishing configuration settings, (4) reinstalling application and system software, and (5) fully testing the system. A full recovery and reconstitution of the information system is performed as part of the Contingency Plan testing.

References:
ARS: CP-10.0
ARS: CP-10.1
HSPD-7: G(22)(i)
NIST 800-53: CP-10
PISP: 4.2.3.10

Related CSRs: 5.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, and application and system software is reinstalled.

Protocols: 1. Examine organizational records or documents to determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system.
2. Examine organizational records or documents to determine if the organization identifies means for capturing the information system's operational state including all system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.
3. Examine organizational records or documents to determine if the organization tests the information system after completion of recovery and reconstitution operations.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system recovery and reconstitution control is implemented.
5. Test recovery and reconstitution mechanisms using selected components of the information system to determine if the system can be fully restored to its original operational state.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts recovery and reconstitution operations on an ongoing basis.
7. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system recovery and reconstitution control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents including results from contingency plan testing to determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

4. Segregation of Duties

4.1 Formal procedures shall guide personnel in performing their security duties.

4.1.1 Detailed, written instructions exist to guide personnel in performing their duties. Computer operator manuals provide guidance on system startup and shutdown procedures, emergency procedures, system and job status reporting, and operator-prohibited activities. Application-specific manuals provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.

References:
ARS: SI-11.0
FISCAM: TSD-3.1.2
HSPD-7: G(22)(i)
NIST 800-53: SI-11
PISP: 4.2.6.11

Related CSRs: 2.1.10, 3.1.3, 3.1.5, 4.2.3, 5.6.3, 9.1.1, 9.3.1, 9.5.1, 9.6.7, 9.6.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Manuals should contain instructions on all procedures which the employee is expected to perform on a regular basis and in an emergency situation.

Protocols: 1. Examine the information system to determine if the system identifies and handles error conditions in an expeditious manner.
2. Examine the information system to determine if the system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries.
3. Examine the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel).
4. Examine the information system to determine if the system lists sensitive information (e.g., account numbers, social security numbers, and credit card numbers) in error logs or associated administrative messages.
5. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the error handling control is implemented.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently handles error conditions on an ongoing basis.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the error handling control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Segregation of Duties***

General Requirement

Control Technique

4.1 Formal procedures shall guide personnel in performing their security duties.

4.1.2 Duties in critical mission functions or sensitive control, financial functions, and information system support functions are divided among separate individuals to ensure least privileged and individual accountability.

References:
ARS: AC-5.CMS-3
CMS: Directed
NIST 800-53: AC-5
PISP: 4.3.2.5

Related CSRs: 4.3.1, 4.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Duties should be documented in job descriptions. Appropriate separation of data will assist in preventing fraud. See BPSSM information on fraud protective measures.

Protocols: 1. Examine organizational records or documents to determine if the information system enforces separation of duties.
2. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
3. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.
5. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

4.1.3 The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.

References:
CMS: Directed
NIST 800-53: CM-4
PISP: 4.2.4.4

Related CSRs: 3.5.2, 10.7.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The approval process should be documented and reviewed periodically.

Protocols: 1. Examine organizational records or documents to determine if the organization monitors changes to the information system and identifies the types of changes monitored.
2. Examine organizational records or documents to determine if the organization performs security impact analyses to assess the effects of changes to the information system.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring configuration changes control is implemented.
4. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently monitors configuration changes to the information system on an ongoing basis.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring configuration changes control are documented and the resulting information used to actively improve the control on a continuous basis.

4.1.4 Operators are prevented from overriding file labels or equipment error messages.

References:
FISCAM: TSD-3.1.4

Related CSRs: 3.1.5, 3.2.2, 9.1.1, 9.3.1, 9.5.1, 9.6.7, 9.6.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: A good approach is to provide periodic training in operating procedures, which should cover operator-prohibited activities.

Protocols: 1. Employees demonstrate that documentation is understood and adhered to.
2. Review documentation describing how controls meet the specified requirement.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

4.1.5 Application-run manuals provide instruction on operating specific applications, including in-house applications.

References:
FISCAM: TSD-3.1.3

Related CSRs: 3.4.3, 6.3.13

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Manuals should include instructions on job setup, console and error messages, job checkpoints, transaction records, and restart and recovery steps after system failure.

Protocols: 1. Employees demonstrate that documentation is understood and adhered to.
2. Inspect run manuals for inclusion of the required instructions.

Category: ***Segregation of Duties***

General Requirement

Control Technique

4.2 Active supervision and review shall be provided for all personnel.

4.2.1 Personnel are provided adequate supervision and review, including each shift of computer operations.

References:
FISCAM: TSD-3.2.1

Related CSRs: 1.4.1, 4.7.4, 7.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Supervision and review of personnel activities assure that these activities are performed in accordance with prescribed procedures, mistakes are corrected, and computers are used for authorized purposes.

Protocols: 1. Review audit data confirming continuing supervision and review in accordance with the documented process.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

4.2.2 All operator activities on the computer system are recorded on an automated history record. Supervisors routinely review the history record and investigate any abnormalities.

References:
FISCAM: TSD-3.2.2
FISCAM: TSD-3.2.3

Related CSRs: 2.1.1, 2.6.1, 3.1.1, 3.1.4, 7.3.4, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The history record serves as an audit record and should be reviewed routinely by supervisors.

Protocols: 1. Interview supervisors to confirm that supervisors routinely review history record.
2. Determine by review that an automated history reocrd exists on each computer system, and that they record all operator activities.
3. Determine, by review supervisor's job description that this is included in the job description.
4. Review history record for signatures indicating supervisory review.
5. Inspect a sample of documentation of the supervisor's investigative process.

4.2.3 System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.

References:
ARS: AC-13.CMS-2
ARS: SI-6.0
FISCAM: TSD-3.2.4
NIST 800-53: AC-13
NIST 800-53: SI-6
PISP: 4.2.6.6
PISP: 4.3.2.13

Related CSRs: 4.1.1, 10.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: IPL establishes the environment in which the computer operates. System startup should be monitored to ensure that security features are enabled.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system verifies the correct operation of security functions upon system startup and restart, and/or upon command by users with appropriate privileges.
2. Interview selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system.
3. Examine organizational records or documents to determine if unusual activity is investigated, reported to appropriate officials, and resolved.
4. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system notifies the system administrator, shuts the system down, or restarts the system when anomalies are discovered.
5. Examine the system configuration to determine if it verifies the correct operations of security functions upon system startup and restart, upon command by user with appropriate privilege, periodically and notifies system administrator, shuts the system down, restarts the system when anomalies are discovered.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security functionality verification control is implemented.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently supervises and reviews user activities with respect to the enforcement and use of access controls for the information system on an ongoing basis.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently verifies the security functionality within the system on an ongoing basis.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the supervision and review of access control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to provide notification of failed security tests to appropriate personnel.
12. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to support management of distributed security testing.

Category: ***Segregation of Duties***

General Requirement

Control Technique

4.3 Job descriptions shall be documented.

4.3.1 Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.

References:
FISCAM: TSD-1.2.1
NIST 800-53: AT-3
PISP: 4.2.9.3

Related CSRs: 3.1.3, 4.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.

Protocols: 1. Examine organizational records or documents to determine if the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities.
2. Examine organizational records or documents to determine if (i) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) the organization provides initial and refresher training in accordance with organization-defined frequency.
3. Examine the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training control is implemented.
5. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently conducts security training on an ongoing basis.
6. Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training control are documented and the resulting information used to actively improve the control on a continuous basis.

4.3.2 Documented job descriptions include definitions of the technical knowledge, skills and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.

References:
FISCAM: TSD-1.2.2

Related CSRs: 5.1.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Confirm by review that job descriptions are documented, and that they meet the specified criteria.

4.4 Management shall review job duties for effectiveness of control techniques.

4.4.1 Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).

References:
FISCAM: TSD-2.2.2

Related CSRs: 2.7.1, 3.1.2, 4.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is a documented management review on an annual basis.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

4.4.2 Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.

References:
FISCAM: TSD-2.2.1

Related CSRs: 3.1.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A periodic employee performance review could be used to demonstrate compliance.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

Category: ***Segregation of Duties***

General Requirement

Control Technique

4.5 Physical and logical access controls shall be established.

4.5.1 Physical and logical access controls restrict employees to authorized actions, based upon organizational and individual job responsibilities.

References:
ARS: AC-5.CMS-2
CMS: Directed
FISCAM: TSD-2.1
NIST 800-53: AC-5
PISP: 4.3.2.5

Related CSRs: 2.3.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities.

Protocols: 1. Examine organizational records or documents to determine if the information system enforces separation of duties.
2. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
3. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.
5. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

4.6 Employees shall understand their security duties and responsibilities.

4.6.1 Security skill needs are accurately identified and included in job descriptions. All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.

References:
FISCAM: TSD-1.3.1
FISCAM: TSP-4.2.1

Related CSRs: 3.1.3, 3.3.3, 3.6.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The SSO should work in conjunction with the HR department on job description updates. Employees should have access to their job descriptions and discuss during their performance evaluations.

Protocols: 1. Interview employees to confirm that their job descriptions match their understanding of their duties and responsibilities, and that they carry out those responsibilities in accordance with their job descriptions.
2. Review a sample of job descriptions for identification of security skills required
3. Evaluate the apparent relevance of the specified security skills to the job described.

4.6.2 Local policy assigns senior management responsibility for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced and institutionalized within the organization.

References:
FISCAM: TSD-1.3.2

Related CSRs: 1.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Senior management is responsible for assuring that employees understand their responsibilities.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

4.6 Employees shall understand their security duties and responsibilities.

4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.

References:
ARS: AC-5.CMS-6
FISCAM: TSD-1.3.3
NIST 800-53: AC-5
PISP: 4.3.2.5

Related CSRs: 3.3.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to develop a matrix identifying resources in relation to organizational access and job title.

Protocols: 1. Examine organizational records or documents to determine if the information system enforces separation of duties.
2. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
3. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.
5. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

4.7 Incompatible duties shall be identified and policies implemented to segregate these duties.

4.7.1 Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

References:
FISCAM: TSD-1.1.4

Related CSRs: 4.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Compensating controls should be documented.

Protocols: 1. Review approval controls.

4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through practices and organizational divisions. No individual has complete control over incompatible transaction processing functions.

References:
FISCAM: TSD-1.1.1
FISCAM: TSD-1.1.3

Related CSRs: 4.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish independent organizational groups with defined functions. Functions and related tasks performed by each unit should be documented. Policies are documented, communicated, and enforced.

Protocols: 1. Confirm by review that the required analyses reflect current operations.
2. Review the required analyses for inclusion of the specified elements.
3. Confirm through inspection that the required policies and procedures exist and are consistent with current operations.

4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.

References:
ARS: SI-9
FISCAM: TSD-1.1.5
NIST 800-53: SI-9
PISP: 4.2.6.9

Related CSRs: 1.5.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Policy procedures and access approvals need to account for correct users of information systems. The initiating approval form can identify job descriptions that are involved for system and application access.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system employs restrictions on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities.
2. Examine the information system to determine if user accounts are restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information input restrictions control is implemented.
4. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently restricts information system inputs to the information system on an ongoing basis.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information input restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Segregation of Duties***

General Requirement

Control Technique

4.7 Incompatible duties shall be identified and policies implemented to segregate these duties.

4.7.4 Day-to-day operating procedures and security controls for the data center are adequately documented and implemented, and prohibited actions are identified.

References:
ARS: PE-3.CMS-4
FISCAM: TSD-1.1.6
NIST 800-53: PE-3
PISP: 4.2.2.3

Related CSRs: 4.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Documentation should be reviewed periodically and updated as needed.

Protocols: 1. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
2. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
3. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls physical access to the facility where the information system resides on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access control are documented and the resulting information used to actively improve the control on a continuous basis.

4.7.5 Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) testing functions (i.e., user acceptance, quality assurance, information security); (6) library management/change management; (7) computer operations; (8) production control and scheduling; (9) data control; (10) data security; (11) data administration; and (12) network administration.

References:
ARS: AC-5.CMS-4
ARS: AC-5.CMS-6
FISCAM: TSD-1.1.2
NIST 800-53: AC-5
PISP: 4.3.2.5

Related CSRs: 3.4.1, 3.4.2, 3.5.1, 3.5.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Manuals and job descriptions include support functions of each individual.

Protocols: 1. Examine organizational records or documents to determine if the information system enforces separation of duties.
2. Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.
3. Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.
5. Test access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Service Continuity***

General Requirement

Control Technique

5. Service Continuity

5.1 Adequate environmental controls shall be implemented.

5.1.1 Environmental controls are monitored and periodically tested. Levels of alert are evaluated and prescribed guidelines for each alert level are evaluated. When necessary, response procedures are implemented and monitored, management is alerted of possible loss of service and/or media, damage is reported, remedial action is provided, and the Contingency Plan is implemented.

References:
FISCAM: TSC-2.2.6

Related CSRs: 5.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be a test plan for the testing of the environmental controls, e.g., humidistat.

Protocols: 1. Review the test plans for future tests.
2. Review documentation supporting recent tests of environmental controls.
3. Review test policies.

5.1.2 Controls have been identified to sufficiently mitigate identified risks and other disasters, such as floods, earthquakes, fire, etc.

References:
FISCAM: TSC-2.2.2

Related CSRs: 1.8.2, 2.2.29, 5.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The SSO should work in conjunction with the building engineer/maintenance. High risk items should be identified e.g., location of the flood plain.

Protocols: 1. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.
2. Review documentation of risk mitigation planning covering all identified risks.
3. Review documentation of efforts to identify additional risks specific to the region, area, or facility.
4. Review the risk assessment plan for consideration of the specified potential risks.

5.1.3 An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down. Where necessary to maintain an operational capability, a redundant and parallel power cabling path, or a long-term alternate power supply is provided for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

References:
ARS: PE-11.1
ARS: PE-9.1
FISCAM: TSC-2.2.5
NIST 800-53: PE-11
NIST 800-53: PE-9
PISP: 4.2.2.11
PISP: 4.2.2.9

Related CSRs: 5.9.7, 5.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The facility managers should periodically verify the current computing power load and auxiliary requirements for change.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss.
2. Examine organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a short-term power supply for the information system.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency power control is implemented.
4. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently provides an emergency power capability for the information system on an ongoing basis.
5. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency power control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
7. Examine organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a long-term alternate power supply for the information system.
8. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.
9. Examine organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a long-term, self-contained alternate power supply for the information system.

5.1 Adequate environmental controls shall be implemented.

5.1.4 Electric power distribution, heating plants, water, sewage, and other utilities are periodically reviewed for risk of failure. Information system power equipment and power cabling are protected from damage and destruction. Only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

References:
ARS: PE-9.CMS-1
HSPD-7: G(22)(i)
NIST 800-53: PE-9
PISP: 4.2.2.9

Related CSRs: 2.2.21, 5.9.14, 10.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be a process for the testing of the environmental controls and periodic reviews for risk of failure.

Protocols: 1. Examine organizational records, documents, and the facility where the information system resides to determine if the organization protects power equipment and power cabling for the information system from damage and destruction.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the power equipment and power cabling control is implemented.
3. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently protects power equipment and power cabling for the information system on an ongoing basis.
4. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the power equipment and power cabling control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examinee organizational records, documents, and the facility where the information system resides to determine if the organization employs redundant and parallel power cabling paths.

5.1.5 A master power switch or emergency cut-off switch is implemented, maintained, and prominently marked and protected by a cover for Data Centers, server, and mainframe rooms. Emergency lighting systems that activate automatically in the event of a power outage or disruption and that cover emergency exits and evacuation routes are implemented and maintained.

References:
ARS: PE-10.CMS-1
ARS: PE-12
NIST 800-53: PE-10
NIST 800-53: PE-12
PISP: 4.2.2.10
PISP: 4.2.2.12

Related CSRs: 2.2.29

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that address these control objectives.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization provides the capability of shutting off power to any information system component that may be malfunctioning or threatened.
2. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains an automatic emergency lighting system that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
3. Examine the emergency shutoff capability to ensure that it exists and is functional.
4. Examine organizational records or documents to determine if the results of the last tested power outage demonstrated that the emergency lighting system was operational and fully functional.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency shutoff control is implemented.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency lighting control is implemented.
7. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization consistently employs an emergency shutoff capability for the information system on an ongoing basis.
8. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization provides and maintains an emergency lighting system for the information system on an ongoing basis.
9. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency shutoff and lighting controls are documented and the resulting information used to actively improve the control on a continuous basis.

5.1 Adequate environmental controls shall be implemented.

5.1.6 Redundancy exists in the air cooling system. Acceptable temperature and humidity levels are maintained and monitored, and specific control alarms within facilities containing information systems are monitored. Levels of alert are evaluated and prescribed guidelines for each alert level are evaluated. When necessary, management is alerted of possible loss of service and/or media, damage is reported, remedial action is provided, and the Contingency Plan is implemented.

References:
ARS: PE-14.CMS-1
ARS: PE-14.CMS-2
ARS: PE-14.CMS-3
FISCAM: TSC-2.2.3
NIST 800-53: PE-14
PISP: 4.2.2.14

Related CSRs: 5.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Only the critical components or subsystems of the entire air cooling system need to be redundant.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization regularly maintains, within acceptable levels, and monitors the temperature and humidity of the facility where the information system resides.
2. Examine the facility where the information system resides to determine if the temperature and humidity controlling systems are in place and functioning as intended.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the temperature and humidity control is implemented.
4. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently maintains and monitors temperature and humidity levels within the facility where the information system resides on an ongoing basis.
5. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the temperature and humidity control are documented and the resulting information used to actively improve the control on a continuous basis.

5.1.7 Fire suppression and detection devices that activate automatically or can be activated in the event of a fire (e.g., fire extinguishers, and sprinkler systems) have been installed and are working. The fire suppression and detection devices are configured to automatically notify emergency responders and the organization upon activation.

References:
ARS: PE-13.1
ARS: PE-13.2
FISCAM: TSC-2.2.1
NIST 800-53: PE-13
PISP: 4.2.2.13

Related CSRs: 5.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to have the fire department review the systems.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.
2. Examine the results of the last test of the fire suppression and detection devices/systems to determine if the fire protection resources can be successfully activated in the event of a fire.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the fire protection control is implemented.
4. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently provides fire suppression and detection devices/systems for the facility where the information system resides on an ongoing basis.
5. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the fire protection control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if fire suppression and detection devices/systems activate automatically in the event of a fire.
7. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if the fire suppression and detection devices/systems for the facility where the information system resides provide automatic notification of any activation to the organization and emergency responders.
8. Examine the alarm system service level agreement to determine if the agreement details automatic notification to the organization and emergency responders.
9. Examine organizational records or documents to determine if the results of the last test of the fire suppression and detection devices/systems demonstrated that the organization and emergency responders were automatically notified.

Category: ***Service Continuity***

General Requirement

Control Technique

5.1 Adequate environmental controls shall be implemented.

5.1.8 Building plumbing lines are known and do not endanger the computer facility or, at a minimum, shutoff valves and their operating procedures exist and are known. Automated mechanisms are implemented to close shutoff valves without manual intervention in the event of a significant water leak.

References:
ARS: PE-15.1
FISCAM: TSC-2.2.4
NIST 800-53: PE-15
PISP: 4.2.2.15

Related CSRs: 5.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The SSO should work in conjunction with the building engineer/maintenance.

Protocols: 1. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization protects the information system from water damage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
2. Examine the facility where the information system resides to determine if the master shut-off valves are accessible and working properly.
3. Examine organizational records or documents to determine if the results of the last test of the environmental controls of the facility where the information system resides demonstrate that the master shut-off valves are working properly.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the water damage protection control is implemented.
5. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently protects the information system from water damage on an ongoing basis.
6. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the water damage protection control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if automated mechanisms and automated functions are employed to automatically close shut-off valves in the event of a significant water leak.
8. Examine the automated mechanisms for water shut-off valves within the facility to determine if each automated function is properly configured to ensure that water valves can be automatically shut off in the event of a significant water leak.

5.1.9 Any behavior that may damage computer equipment is prohibited. Power surge protection is implemented for all computer equipment.

References:
ARS: PE-CMS-1.CMS-1
FISCAM: TSC-2.2.7
PISP: 4.2.2.1

Related CSRs: 4.3.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Management should include behavioral guidance. For example keeping cans of coke on top of a PC could damage it.

Protocols: 1. Review job descriptions to ensure there is guidance contained relative to destructive behavior.
2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment.
3. Review the risk assessment for identification of potentially hazardous employee activities.

Category: ***Service Continuity***

General Requirement

Control Technique

5.2 A Contingency Plan shall be documented in accordance with the CMS Business Partners Systems Security Manual.

5.2.1 Contingency Plans consist of all components listed in the CMS Business Partners Systems Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

References:
ARS: CP-2.1
ARS: CP-3.0
ARS: CP-3.1
ARS: CP-5.0
CMS: Directed
FISCAM: TSC-3.1.1
HIPAA: 164.308(a)(7)(i)
HIPAA: 164.308(a)(7)(ii)(A)
HIPAA: 164.308(a)(7)(ii)(C)
HIPAA: 164.308(a)(7)(ii)(D)
HIPAA: 164.308(a)(7)(ii)(E)
HIPAA: 164.310(d)(1)
NIST 800-53: CP-2
NIST 800-53: CP-3
NIST 800-53: CP-5
PISP: 4.2.3.2
PISP: 4.2.3.3
PISP: 4.2.3.5

Related CSRs: 3.6.7, 5.1.6, 5.3.1, 5.4.3, 5.4.5, 5.5.1, 5.6.1, 5.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A business partner Contingency Plan contains the topics described in Appendix B of the Business Partners Systems Security Manual. Development of the Contingency Plan is coordinated with parties responsible for related plans, such as the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan and Incident Response Plan.

Protocols: 1. Review Appendix B of the Business Partners Systems Security Manual.
2. Examine organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.
3. Examine the contingency plan for the information system to determine if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST SP 800-34.
4. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis.
7. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans.

5.2.2 Management, the SSO, and key affected parties approve Contingency Plans.

References:
CMS: Directed
FISCAM: TSC-3.1.1
NIST 800-53: CP-2
PISP: 4.2.3.2

Related CSRs: 5.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that the Contingency Plan be reviewed and approved by persons that are knowledgeable about the systems and environment so that nothing is missed in the plan.

Protocols: 1. Examine organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.
2. Examine the contingency plan for the information system to determine if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST SP 800-34.
3. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis.

Category: ***Service Continuity***

General Requirement

Control Technique

5.2 A Contingency Plan shall be documented in accordance with the CMS Business Partners Systems Security Manual.

5.2.3 Management and the SSO are able to show how the organization responds to specific disasters/disruptions to: (1) protect lives, (2) limit damage, (3) protect sensitive data, (4) circumvent safeguards according to established bypass procedures, and (5) minimize the impact on Medicare operations.

References:
CMS: Directed
FISCAM: TSC-3.1.1

Related CSRs: 2.6.2, 5.5.1, 5.6.1, 5.6.2, 5.6.3, 5.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach might be to review documentation in the security profile to determine if the organization has responded properly to emergency situations (such as incidents) in the past.

Protocols: 1. Review documentation, CCTV tapes or other recordings.
2. Determine through interview that system manager(s) and the SSO can explain how the organization covers each of the specified requirements through its response to specific disasters/disruptions.

5.2.4 The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.

References:
CMS: Directed

Related CSRs: 5.3.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Critical interfaces should be tested when the contingency plan is exercised.

Protocols: 1. Review test reports.
2. Verify through inspection that the contingency plan identifies the specified interfaces.

5.2.5 The Contingency Plan clearly assigns responsibilities for recovery and provides for backup personnel so that it can be implemented independent of specific individuals.

References:
FISCAM: TSC-3.1.1
FISCAM: TSC-3.1.2
NIST 800-53: CP-2
PISP: 4.2.3.2

Related CSRs: 3.6.4, 4.3.1, 4.6.1, 5.6.1, 5.8.1, 5.10.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that individuals have been assigned to all the responsibilities that need to be executed during a contingency. Refer to Appendix B of the BPSSM.

Protocols: 1. Examine organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.
2. Examine the contingency plan for the information system to determine if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST SP 800-34.
3. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented.

5.2.6 The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.

References:
CMS: Directed
HIPAA: 164.308(a)(7)(ii)(C)

Related CSRs: 2.2.5, 2.4.1, 2.4.2, 5.6.1, 5.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that this immediate entry action has been practiced during exercises and training.

Protocols: 1. Review the Contingency Plan emergency response procedures for inclusion of the required provision.

5.2.7 Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency Plans are re-evaluated before proposed changes are approved.

References:
CMS: Directed

Related CSRs: 5.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Change control management should provide for updates to the Contingency Plan.

Protocols: 1. Review audit data confirming that contingency plans have been reevaluated before any proposed major modifications were approved.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.2 A Contingency Plan shall be documented in accordance with the CMS Business Partners Systems Security Manual.

5.2.8 Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.

References:
CMS: Directed
HSPD-7: G(22)(i)

Related CSRs: 2.5.1, 2.14.2, 3.6.6, 5.11.2, 6.4.2, 7.2.2, 9.3.3, 9.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Throughout documentation review and testing, ensure that the safeguards protect data from modification if the system fails.

Protocols: 1. Review documentation describing use of software procedures to reduce the potential for data loss and/or modification during a system failure.
2. Review documentation describing use of installed security and backup capabilities to reduce the potential for data loss and/or modification during a system failure.
3. Review documentation supporting the contention that existing contingency plans protect storage media from improper modification in the event of system failure.

5.2.9 User departments have developed adequate manual processing procedures for use until automated operations are restored.

References:
FISCAM: TSC-3.1.3

Related CSRs: 1.8.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Determine that the manual procedures have been tested. Refer to Appendix B of the BPSSM.

Protocols: 1. Review test reports to determine that manual procedures have been tested, at least on a sample basis.
2. Interview the relevant process managers to confirm familiarity with the required procedures.
3. Inspect the required manual procedures for consistency with the contingency plan.
4. Review the contingency plan for identification of the specified manual procedures.
5. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation.

5.3 Critical data and operations shall be identified and prioritized.

5.3.1 A list of critical applications, operations and data has been documented that: (1) prioritizes data and operations; (2) is approved by senior program managers; and (3) reflects current conditions.

References:
FISCAM: TSC-1.1
HIPAA: 164.308(a)(7)(ii)(E)

Related CSRs: 1.8.3, 2.1.5, 5.2.4, 5.4.1, 5.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important to know what critical data and operations are needed to continue critical functions in an emergency.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation supporting the contention that the list reflects current conditions.
3. Verify by inspection that the list is approved by senior management.
4. Verify by inspection that the required, prioritized list has been prepared.

5.4 Data and program backup procedures shall be implemented.

5.4.1 The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.

References:
CMS: Directed
HIPAA: 164.308(a)(7)(ii)(A)
HIPAA: 164.310(d)(1)

Related CSRs: 5.11.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Refer to Appendix B of the BPSSM.

Protocols: 1. Observe the initiation of delivery of critical data from the primary site to the off-site facility.
2. Review records of data backups.
3. Review the Contingency Plan to verify that it contains the specified elements.

5.4.2 A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.

References:
HIPAA: 164.310(d)(2)(iv)

Related CSRs: 2.2.23

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A record should be use to track the movement all resources.

Protocols: 1. An inventory of all equipment and software should be maintained, including the location and person responsible.

5.4 Data and program backup procedures shall be implemented.

5.4.3 System and application documentation are maintained at the off-site storage location.

References:
ARS: CP-7.0
FISCAM: TSC-2.1.2
NIST 800-53: CP-7
PISP: 4.2.3.7

Related CSRs: 5.7.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Current systems and applications documentation should be available off-site in case the primary processing site is disabled.

Protocols: 1. Examine the alternate processing site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate processing site control is implemented.
3. Examine the alternate processing site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.

5.4.4 The backup storage and alternate processing sites are identified in the Contingency Plan, and are geographically removed from the primary site(s) and protected by environmental controls and physical access controls. The backup storage and alternate processing sites are located at least 100 miles from the primary processing site.

References:
ARS: CP-6.1
ARS: CP-7.1
FISCAM: TSC-2.1.3
NIST 800-53: CP-6
NIST 800-53: CP-7
PISP: 4.2.3.6
PISP: 4.2.3.7

Related CSRs: 5.10.3, 5.11.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It should be verified that the backup and alternate processing sites are geographically removed from the primary site and are protected by environmental and physical access controls.

Protocols: 1. Examine organizational records or documents to determine if alternate storage site agreements are currently in place to permit storage of information system backup information.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate storage site control is implemented.
3. Examine the alternate storage site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information.
4. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates alternate storage site agreements on an ongoing basis.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate storage sites control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine the alternate storage site to determine if the site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.
7. Examine the alternate storage site agreement to determine if the agreement specifies requirements to facilitate timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives).
8. Test the alternate storage site operations to determine if the site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreement.
9. Examine the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.

Category: ***Service Continuity***

General Requirement

Control Technique

5.4 Data and program backup procedures shall be implemented.

5.4.5 Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged. Backup information is tested for media reliability and information integrity after each backup. Select backup information is used to restore information systems as part of the Contingency Plan testing.

Related CSRs: 5.9.7, 5.11.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: CP-9.0
ARS: CP-9.1
ARS: CP-9.2
FISCAM: TSC-2.1.1
HIPAA: 164.308(a)(7)(ii)(B)
NIST 800-53: CP-9
PISP: 4.2.3.9

Guidance: Offsite backup files should be current to the point that operations would not be delayed or disrupted if the data or software were suddenly put into operation.

Protocols: 1. Examine organizational records or documents to determine if the organization defines the user-level and system-level information (including system state information) that is required to be backed up and identifies the location for storing backup information.
2. Examine selected information system backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup control is implemented.
4. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts information system backups on an ongoing basis.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system backup control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity.
7. Examine organizational records or documents to determine if the organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing and if the use of the backup information contributes to a successful restoration of the identified functions within the information system.
8. Examine the storage location for backup copies of the operating system and other critical information system software to determine if the backup copies of the software are stored in a separate facility or in afire-rated container that is not collocated with the operational software.
9. Examine organizational records or documents to determine if copies of backup information are encrypted.
10. Test the mechanisms used to encrypt backup information on the information system by selectively decrypting selected backup files and comparing the plain text to original backup information.

5.4 Data and program backup procedures shall be implemented.

5.4.6 Incremental backups are performed daily, and full backups are performed weekly. Three generations of backups are stored off site. Both off-site and on-site backups are recorded with name, date, time, and action. Backup copies of the operating system and other critical information system software are protected from unauthorized modification and stored at a separate facility or in a fire-rated container that is not collocated with operational software.

References:
ARS: CP-9.0
ARS: CP-9.3
ARS: MP-4.CMS-1
ARS: MP-4.CMS-2
NIST 800-53: CP-9
NIST 800-53: MP-4
PISP: 4.2.3.9
PISP: 4.2.7.4

Related CSRs: 1.3.10

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Off-site backup files should be current such that operations would not be delayed or disrupted beyond acceptable time limits in the event it becomes necessary to operate using the backup data or software.

Protocols: 1. Examine organizational records or documents to determine if the organization defines the user-level and system-level information (including system state information) that is required to be backed up and identifies the location for storing backup information.
2. Examine selected information system backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures.
3. Examine organizational records or documents to determine if the organization protects information system media at the highest FIPS 199 security category for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures.
4. Examine the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup and media storage controls are implemented.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts information system backups on an ongoing basis.
7. Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis.
8. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system backup and media storage controls are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity.
10. Examine organizational records or documents to determine if the organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing and if the use of the backup information contributes to a successful restoration of the identified functions within the information system.
11. Examine the storage location for backup copies of the operating system and other critical information system software to determine if the backup copies of the software are stored in a separate facility or in afire-rated container that is not collocated with the operational software.
12. Examine organizational records or documents to determine if copies of backup information are encrypted.
13. Test the mechanisms used to encrypt backup information on the information system by selectively decrypting selected backup files and comparing the plain text to original backup information.

5.5 Emergency processing priorities shall be established.

5.5.1 Emergency processing priorities have been documented and approved by appropriate program and data processing managers.

References:
FISCAM: TSC-1.3
HIPAA: 164.308(a)(7)(ii)(C)

Related CSRs: 5.3.1, 5.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Processing priorities should exist for all critical functions and processes to be accomplished during an emergency. These should be periodically reviewed for accuracy.

Protocols: 1. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.6 Management and staff shall be trained to respond to emergencies.

5.6.1 Employees have received training and understand their emergency roles and responsibilities. Simulated events are incorporated into contingency training to facilitate effective response by personnel in crisis situations. Automated mechanisms are employed to provide thorough and realistic training environments.

References:
ARS: CP-3.1
ARS: CP-3.2
FISCAM: TSC-2.3.1
NIST 800-53: CP-3
PISP: 4.2.3.3

Related CSRs: 5.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be evidence that the employees have periodically received training relative to what to do in an emergency.

Protocols: 1. Examine organizational records or documents to determine if the organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities.
2. Examine organizational records or documents to determine if the organization: (i) provides contingency training to personnel with significant contingency roles and responsibilities or personnel implementing the contingency plan; (ii) records the type of contingency training received and the date completed; and (iii) provides initial and refresher training in accordance with organization-defined frequency, at least annually.
3. Examine the contingency training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency training control is implemented.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts contingency training on an ongoing basis.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency training control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization simulates contingency training events.
8. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the organization uses simulated events to improve the training process.
9. Test selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation.
10. Examine organizational records or documents to determine if the organization employs automated mechanisms to improve contingency training.
11. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the training process.
12. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

5.6.2 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.

References:
FISCAM: TSC-2.3.2

Related CSRs: 1.6.4, 5.1.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: These are procedures primarily for staff and management working in a data processing center environment.

Protocols: 1. Review training plans for future training in emergency actions.
2. Review training records to confirm that the required training has been delivered periodically.

5.6.3 Training in emergency procedures is conducted at least once a year and emergency procedures are periodically tested.

References:
CMS: Directed
FISCAM: TSC-2.3.3
FISCAM: TSC-2.3.4
HIPAA: 164.308(a)(7)(i)
HIPAA: 164.308(a)(7)(ii)(C)
HIPAA: 164.308(a)(7)(ii)(D)

Related CSRs: 2.2.29, 2.4.1, 4.1.1, 5.1.7, 5.2.6, 5.5.1, 5.7.1, 6.1.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Emergency procedures should be defined in a procedure manual as part of the Contingency Plan and training performed annually. A record should be maintained that verifies that the training took place. Procedures for use during an emergency situation should be tested annually, or whenever major changes are made to the system environment. Refer to Appendix B of the BPSSM.

Protocols: 1. Review future test plans to ensure that the emergency procedures are scheduled to be properly tested.
2. Interview data center staff.
3. Review documentation confirming completion of the required testing.
4. Review relevant policies and procedures for inclusion and directed use of the required process.
5. Verify the emergency procedures are dealt with in the COOP.
6. By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan.

5.7 The Contingency Plan shall be annually reviewed and tested.

5.7.1 The current Contingency Plan is executable and tested annually using a combination of tabletop exercises and operational tests under conditions that simulate an emergency or a disaster. Automated mechanisms are employed to more thoroughly and effectively test and/or exercise the contingency plan. The Contingency Plan is tested and/or exercised at the alternate processing site to evaluate the site's capabilities to support contingency operations. Testing and/or exercising of the contingency plan is coordinated with parties responsible for related plans, such as: (1) Business Continuity Plan, (2) Disaster Recovery Plan, (3) Continuity of Operations Plan, (4) Business Recovery Plan, and (5) Incident Response Plan.

References:

ARS: CP-4.1
ARS: CP-4.2
ARS: CP-4.3
ARS: CP-5.0
CMS: Directed
FISCAM: TSC-4.1
HIPAA: 164.308(a)(7)(ii)(D)
NIST 800-53: CP-4
NIST 800-53: CP-5
PISP: 4.2.3.4
PISP: 4.2.3.5

Related CSRs: 2.5.8, 5.6.1, 5.6.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is advisable to conduct "live tests" of critical system processes to ensure they will function in an emergency.

Protocols:
1. Examine organizational records or documents to determine if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests.
2. Examine organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually.
3. Examine organizational records or documents to determine if the organization reviews the contingency plan test results and takes corrective actions.
4. Examine the contingency plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.
5. Examine organizational records or documents to determine if the contingency plan tests or exercises address key aspects of the plan and if the tests or exercises confirm that the plan objectives are met.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan testing and updating controls are implemented.
7. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis.
8. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan.
9. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts contingency plan testing on an ongoing basis.
10. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan update and testing controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Examine organizational records or documents to determine if the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
12. Examine organizational records or documents to determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.
13. Examine organizational records or documents to determine if the organization employs automated mechanisms for contingency testing.
14. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the testing process.
15. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

5.7 The Contingency Plan shall be annually reviewed and tested.

5.7.2 Contingency Plans and associated documentation are reviewed and, if required, updated whenever new operations are planned or new safeguards contemplated. Contingency Plans must be updated minimally at least every 3 years. The Disaster Recovery Plan is current and executable, and it is tested and/or exercised once per year or when a major change is made to ensure proper functionality.

Related CSRs: 1.9.9, 1.12.3, 3.5.5, 5.2.7, 6.3.14

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: CP-4.0
ARS: CP-5.0
ARS: CP-CMS-1.1
CMS: Directed
FISCAM: TSC-3.1.1
NIST 800-53: CP-4
NIST 800-53: CP-5
PISP: 4.2.3.11
PISP: 4.2.3.4
PISP: 4.2.3.5

Guidance: Contingency plans should be reviewed before system or process changes are made to determine the possible changes necessary to the Contingency Plan. Change Control Management should alert the contingency plan team to all changes.

Protocols: 1. Examine organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually.
2. Examine organizational records or documents to determine if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests.
3. Examine organizational records or documents to determine if the organization reviews the contingency plan test results and takes corrective actions.
4. Examine organizational records or documents to determine if the contingency plan tests or exercises address key aspects of the plan and if the tests or exercises confirm that the plan objectives are met.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan testing control is implemented.
6. Examine the contingency plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan update control is implemented.
8. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan.
9. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts contingency plan testing on an ongoing basis.
10. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis.
11. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan testing and update controls are documented and the resulting information used to actively improve the control on a continuous basis.
12. Examine organizational records or documents to determine if the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
13. Examine organizational records or documents to determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.
14. Examine organizational records or documents to determine if the organization employs automated mechanisms for contingency testing.
15. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the testing process.
16. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

5.7 The Contingency Plan shall be annually reviewed and tested.

5.7.3 Several copies of the current Contingency Plan are securely stored off-site at different locations, including homes of key staff members. It is reviewed once a year, reassessed and, if appropriate, revised to reflect changes in hardware, software and personnel.

References:
ARS: CP-5.0
CMS: Directed
FISCAM: TSC-3.1.1
FISCAM: TSC-3.1.4
FISCAM: TSC-3.1.5
NIST 800-53: CP-2
NIST 800-53: CP-5
PISP: 4.2.3.5

Related CSRs: 5.4.3, 5.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Current contingency plans should be readily available to key persons during an emergency. Off-site storage will help ensure this availability.

Protocols: 1. Examine organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.
2. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan.
3. Examine organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis.
7. Examine organizational records or documents to determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans.

5.7.4 Test and/or exercise results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.

References:
FISCAM: TSC-4.2.1
NIST 800-53: CP-4

Related CSRs: 3.5.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Senior management should be informed in a timely manner of contingency plan test results and lessons learned so that they can direct appropriate actions to modify the plan or change test plans and procedures.

Protocols: 1. Examine organizational records or documents to determine if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests.
2. Examine organizational records or documents to determine if the organization reviews the contingency plan test results and takes corrective actions.
3. Examine organizational records or documents to determine if the contingency plan tests or exercises address key aspects of the plan and if the tests or exercises confirm that the plan objectives are met.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan testing control is implemented.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts contingency plan testing on an ongoing basis.
7. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan testing control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
9. Examine organizational records or documents to determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.
10. Examine organizational records or documents to determine if the organization employs automated mechanisms for contingency testing.
11. Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the testing process.
12. Test selected automated mechanisms to determine if the mechanisms are operating as intended.

5.7 The Contingency Plan shall be annually reviewed and tested.

5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing and/or exercising.

References:
ARS: CP-4.0
ARS: CP-5.0
FISCAM: TSC-4.2.2
HIPAA: 164.308(a)(7)(ii)(D)
NIST 800-53: CP-4
NIST 800-53: CP-5
PISP: 4.2.3.4
PISP: 4.2.3.5

Related CSRs: 1.11.5, 5.10.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Following contingency plan testing it is advisable to review the test results and make modifications to the plan and related agreements with inside and outside organizations as quickly as possible.

Protocols: 1. Review documents establishing that the contingency plan and related agreements are adjusted as specified.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.8 Resources supporting critical operations shall be identified.

5.8.1 Key resources supporting critical and sensitive operations are identified and documented. Types of key resources identified include: (1) computer hardware; (2) computer software; (3) computer supplies; (4) system documentation; (5) telecommunications; (6) office facilities and supplies; and (7) human resources.

References:
ARS: CP-7.0
FISCAM: TSC-1.2
HSPD-7: D(8)
HSPD-7: E(12)
HSPD-7: F(19)(c)
HSPD-7: G(24)
HSPD-7: H(25)(a)
HSPD-7: J(27)(a)
HSPD-7: J(27)(b)
NIST 800-53: CP-7
PISP: 4.2.3.7

Related CSRs: 2.1.5, 3.4.3, 5.2.5, 5.3.1, 5.4.1, 5.9.7, 5.10.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that resources needed to support critical and sensitive operations during an emergency and recovery time periods be documented for availability to all concerned persons, and that they be reviewed for currency whenever the contingency plan is to be tested.

Protocols: 1. Examine organizational records or documents to determine if alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate processing site control is implemented.
3. Examine the alternate processing site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.
4. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates alternate processing site agreements on an ongoing basis.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate processing sites control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine the contingency plan to determine if the plan identifies the primary processing site hazards.
7. Examine the alternate processing site to determine if the site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.
8. Examine the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.
9. Examine alternate processing site agreements to determine if the agreements contain priority of service provisions in accordance with the organization's availability requirements.
10. Examine alternate processing site agreements to determine if the agreements specify the requirements needed to support the minimum required operational capability of the organization.
11. Test selected components of the information system at the alternate processing site to determine if the site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.1 Goals are established by senior management for the availability of data processing and on-line services. Senior management periodically: (1) reviews and compares the service performance achieved with the goals; and (2) surveys user departments to see if their needs are being met.

References:
FISCAM: TSC-2.4.6
FISCAM: TSC-2.4.9

Related CSRs: 1.11.5, 10.2.9, 10.2.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Reasonable data processing goals should be set by management to guide the maintenance and problem analysis relative to hardware performance and availability. To avoid a break in continuity of service, hardware performance should be evaluated frequently and users polled relative to level of service provided.

Protocols:
1. Interview users.
2. Review the performance records to ensure the goals are clearly stated in writing.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Review documentation confirming establishment of the required goals.

5.9.2 Records are maintained on the actual hardware performance in meeting service schedules.

References:
FISCAM: TSC-2.4.7

Related CSRs: 1.11.5, 10.2.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Records should be kept for all critical hardware components in the system, such as mainframe, server, disc unit, tape unit, controllers, front end processors, and operations consoles and workstations.

Protocols:
1. Inspect the required records.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.9.3 Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.

References:
FISCAM: TSC-2.4.11

Related CSRs: 5.7.3, 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Notice of at least 2 days should be given to users relative to hardware changes.

Protocols:
1. Review records of past advanced notifications.
2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

5.9.4 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.

References:
FISCAM: TSC-2.4.10

Related CSRs: 1.9.4, 3.4.4, 5.7.3, 6.3.13, 6.6.1, 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Any changes to hardware equipment or software should be carefully reviewed, tested, and a schedule created for implementation of the changes. Peak workload periods should be avoided for implementation. Vendor supplied specifications normally prescribe the frequency and type of preventative maintenance to be performed.

Protocols:
1. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.9.5 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.

References:
FISCAM: TSC-2.4.4

Related CSRs: 2.2.24

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: The operational flow of business functions should be designed to permit unscheduled interruptions without adversely affecting critical processes and deliveries.

Protocols:
1. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.6 Routine and preventive maintenance on information system components is scheduled and performed in accordance with manufacturer or vendor specifications and in a manner that minimizes the impact on operations.

References:
ARS: MA-2.2
FISCAM: TSC-2.4.2
NIST 800-53: MA-2
PISP: 4.2.5.2

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Maintenance schedules should be distributed and kept at different locations in the enterprise.

Protocols: 1. Examine organizational records or documents to determine if the organization schedules and performs routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
2. Examine organizational records or documents to determine if the organization fully documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational periodic maintenance requirements.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the periodic maintenance control is implemented.
4. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization conducts periodic maintenance on an ongoing basis.
5. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the periodic maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine the maintenance log to determine if the log includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).
7. Examine the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that periodic maintenance is scheduled and conducted as required.
8. Examine the log of maintenance actions to determine if the log is up to date, accurate, complete, and available.

5.9.7 Maintenance support and spare parts is used to provide a high level of system availability for critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within 24 hours of failure.

References:
ARS: MA-6.0
FISCAM: TSC-2.4.5
NIST 800-53: MA-6
PISP: 4.2.5.6

Related CSRs: 5.4.4, 5.4.5, 5.10.1, 5.11.1, 5.11.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: In an emergency, or for unscheduled maintenance, spare and backup hardware units, and the appropriate switchover software, should be available to prevent interruption of critical processes.

Protocols: 1. Examine organizational records or documents to determine if maintenance support agreements and the inventory of spare parts are sufficient to support the organization-defined list of key information system components within the organization-defined time period of failure.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the timely maintenance control is implemented.
3. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently obtains timely maintenance for the information system on an ongoing basis.
4. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the timely maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.8 Regular and unscheduled hardware maintenance performed is documented. The maintenance record for each system includes: (1) date and time of maintenance; (2) name of the individual performing the maintenance; (3) name of escort, if applicable; (4) description of the maintenance performed; and (5) list of equipment removed or replaced (including identification numbers, if applicable).

References:
ARS: MA-2.1
ARS: MA-2.2
FISCAM: TSC-2.4.3
NIST 800-53: MA-2
PISP: 4.2.5.2

Related CSRs: 1.8.2, 1.9.9, 2.2.27

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Maintenance records are kept and reviewed for trends and lessons learned. They can be organized by type unit or subsystem. Review meetings should be held with major vendors reviewing the statistics.

Protocols: 1. Examine organizational records or documents to determine if the organization schedules and performs routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
2. Examine organizational records or documents to determine if the organization fully documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational periodic maintenance requirements.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the periodic maintenance control is implemented.
4. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization conducts periodic maintenance on an ongoing basis.
5. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the periodic maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine the maintenance log to determine if the log includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).
7. Examine the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that periodic maintenance is scheduled and conducted as required.
8. Examine the log of maintenance actions to determine if the log is up to date, accurate, complete, and available.

5.9.9 Measures and automated mechanisms are employed to ensure that maintenance is scheduled and conducted as required, and that a record of maintenance actions, both needed and complete, is up-to-date, accurate, and readily available. Automated mechanisms are employed to ensure only authorized personnel use maintenance tools. Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information, or maintenance personnel are supervised during the performance of maintenance activities when they do not have the needed access authorizations.

References:
ARS: MA-2.2
ARS: MA-5.0
FISCAM: TSC-2.4.1
NIST 800-53: MA-2
NIST 800-53: MA-5
PISP: 4.2.5.2
PISP: 4.2.5.5

Related CSRs: 1.4.1, 1.8.2, 1.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Protocols: 1. Examine organizational records or documents to determine if the organization schedules and performs routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
2. Examine organizational records or documents to determine if: (i) the organization maintains a list of personnel authorized to perform maintenance on the information system; and (ii) only authorized personnel have performed maintenance on the information system.
3. Examine organizational records or documents to determine if the organization fully documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational periodic maintenance requirements.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the periodic maintenance and maintenance personnel controls are implemented.
5. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization conducts periodic maintenance on an ongoing basis.
6. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently performs an authorization of maintenance personnel on an ongoing basis.
7. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the periodic maintenance and maintenance personnel controls are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine the maintenance log to determine if the log includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).
9. Examine the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that periodic maintenance is scheduled and conducted as required.
10. Examine the log of maintenance actions to determine if the log is up to date, accurate, complete, and available.

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.10 The use of system maintenance tools is approved, controlled, and monitored; and the tools are maintained on an on-going basis. All maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel are inspected for obvious improper modifications. The use of remote diagnostic tools is documented in the SSP. All media containing diagnostic programs is checked for malicious code before the media is used in the system.

References:
ARS: MA-3.1
ARS: MA-3.2
ARS: MA-3.4
ARS: MA-4.2
NIST 800-53: MA-3
NIST 800-53: MA-4
PISP: 4.2.5.3
PISP: 4.2.5.4

Related CSRs: 5.12.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Protocols: 1. Examine organizational records or documents to determine if the organization approves, controls, and monitors information system maintenance tools, and remotely executed maintenance and diagnostic activities.
2. Examine approved information system maintenance tools and associated documentation to determine if the organization maintains the tools and documentation on an ongoing basis and if the processes applied are consistent with the documented maintenance procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote maintenance control is implemented.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance tools control is implemented.
5. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently manages system maintenance tools and remote maintenance on an ongoing basis.
6. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the maintenance tools and remote maintenance controls are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with information system maintenance responsibilities to determine if the organization inspects all maintenance tools used by maintenance personnel for improper modifications.
8. Examine organizational records or documents to determine if the organization inspects selected maintenance tools used by maintenance personnel to ensure that no improper modifications have been made.
9. Interview selected organizational personnel with information system maintenance responsibilities to determine how the organization checks media containing diagnostic test programs for malicious code.
10. Examine organizational records or documents to determine if the organization checks for malicious code on all media containing diagnostic test programs before use within the information system.
11. Examine organizational records or documents to determine if the organization checks all maintenance equipment to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release.
12. Examine selected maintenance equipment that cannot be sanitized to ensure that the equipment is stored in a safe and secure location within the facility or is completely destroyed.
13. Examine organizational records or documents that indicate when maintenance equipment with organization information is removed from the facility that an organizational official explicitly authorizes the equipment removal.
14. Examine organizational records or documents to determine if: (i) the organization audits all remote maintenance sessions and (ii) appropriate organizational personnel review the audit logs of the remote sessions.
15. Examine organizational records or documents to determine if the organization uses automated mechanisms to control access to maintenance tools and if only authorized personnel have access to those tools.
16. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to ensure that only authorized personnel access maintenance tools.
17. Examine organizational records or documents to determine if the organization addresses the installation and use of remote diagnostic links for the information system.
18. Examine the security level of the organization performing remote diagnostic or maintenance services to determine if the services performed are at an acceptable security level.

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.11 All maintenance equipment with the capability of retaining information is checked to ensure that no sensitive information is saved on the equipment and that the equipment is appropriately sanitized prior to release. If the equipment cannot be sanitized, the equipment must remain within the facility or must be destroyed, unless an exception is specifically authorized by the SSO.

References:
ARS: MA-3.3
NIST 800-53: MA-3
PISP: 4.2.5.3

Related CSRs: 1.3.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Protocols: 1. Examine organizational records or documents to determine if the organization approves, controls, and monitors information system maintenance tools.
2. Examine approved information system maintenance tools and associated documentation to determine if the organization maintains the tools and documentation on an ongoing basis and if the processes applied are consistent with the documented maintenance procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance tools control is implemented.
4. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently manages system maintenance tools on an ongoing basis.
5. Interview selected organizational personnel with information system maintenance responsibilities to determine if the organization inspects all maintenance tools used by maintenance personnel for improper modifications.
6. Examine organizational records or documents to determine if the organization inspects selected maintenance tools used by maintenance personnel to ensure that no improper modifications have been made.
7. Examine organizational records or documents to determine if the organization checks all maintenance equipment to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release.
8. Examine selected maintenance equipment that cannot be sanitized to ensure that the equipment is stored in a safe and secure location within the facility or is completely destroyed.
9. Examine organizational records or documents that indicate when maintenance equipment with organization information is removed from the facility that an organizational official explicitly authorizes the equipment removal.
10. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to ensure that only authorized personnel access maintenance tools.

5.9.12 If the remote diagnostic or maintenance service organization does not have a system level of security at least as high as the system being serviced, the information system being serviced is sanitized and physically disconnected from other information systems prior to allowing a remote connection. Before the service begins, the information system is sanitized (with regard to CMS sensitive information) and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system. If the system cannot be sanitized (e.g., due to a system failure), remote maintenance is not permitted.

References:
ARS: MA-4.0
ARS: MA-4.3
NIST 800-53: MA-4
PISP: 4.2.5.4

Related CSRs: 1.3.4, 2.8.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Protocols: 1. Examine organizational records or documents to determine if the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote maintenance control is implemented.
3. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently approves, monitors, and controls remote maintenance on an ongoing basis.
4. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Examine organizational records or documents to determine if: (i) the organization audits all remote maintenance sessions and (ii) appropriate organizational personnel review the audit logs of the remote sessions.
6. Examine organizational records or documents to determine if the organization addresses the installation and use of remote diagnostic links for the information system.
7. Examine the security level of the organization performing remote diagnostic or maintenance services to determine if the services performed are at an acceptable security level.

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.13 Remote diagnostic or maintenance service organizations are required to utilize a system level of security at least as high as the system being serviced. All remote maintenance and diagnostic sessions are audited and appropriate CMS information security personnel review the audit records of the remote sessions. Maintenance and diagnostic communications are encrypted and decrypted; strong identification and authentication techniques are used, such as tokens; and all sessions and remote connections are terminated when remote maintenance is completed. If password-based authentication is used during remote maintenance and diagnostic sessions, passwords are changed following each remote maintenance and diagnostic service.

References:
ARS: MA-4.0
ARS: MA-4.1
ARS: MA-4.3
NIST 800-53: MA-4
PISP: 4.2.5.4

Related CSRs: 2.8.5, 10.8.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Protocols: 1. Examine organizational records or documents to determine if the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote maintenance control is implemented.
3. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently approves, monitors, and controls remote maintenance on an ongoing basis.
4. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Examine organizational records or documents to determine if: (i) the organization audits all remote maintenance sessions and (ii) appropriate organizational personnel review the audit logs of the remote sessions.
6. Examine organizational records or documents to determine if the organization addresses the installation and use of remote diagnostic links for the information system.
7. Examine the security level of the organization performing remote diagnostic or maintenance services to determine if the services performed are at an acceptable security level.

5.9.14 On-site repair of servers is performed within protected environments. Access to system for repair is by authorized personnel only. For off-site repair of systems, off-site access to the systems is performed by authorized personnel only. Electronic storage media is removed before shipment for repairs. Unusable electronic storage media is sanitized or destroyed by authorized personnel. After maintenance is performed, security features are checked to ensure they are functioning properly.

References:
ARS: MA-CMS-1.CMS-1
ARS: MA-CMS-2.CMS-1
ARS: MA-CMS-2.CMS-2
PISP: 4.2.5.1

Related CSRs: 1.3.4, 2.2.31, 5.1.4, 10.1.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Protocols: 1. Review documentation supporting the contention that the required policies and procedures are up-to-date.
2. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.

5.9.15 Problems and delays encountered, including the reason and elapsed time for resolution of hardware problems, are recorded and analyzed to identify recurring patterns or trends.

References:
FISCAM: TSC-2.4.8

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Hardware problems should be carefully analyzed in order to determine the maintenance needs and to prevent major failures.

Protocols: 1. Review documentation supporting conduct of the required analyses.
2. Review samples of the required records.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

5.10 Arrangements shall be made for alternate data processing and telecommunications facilities.

5.10.1 Arrangements and agreements have been established for a backup data center and other needed facilities that: (1) are in a state of readiness commensurate with the risks of interrupted operations; (2) have sufficient processing capacity and; (3) are available for use.

References:
ARS: CP-7.0
ARS: CP-7.3
ARS: CP-7.4
ARS: CP-8.0
ARS: CP-8.1
CMS: Directed
FISCAM: TSC-3.2.1
NIST 800-53: CP-7
NIST 800-53: CP-8
PISP: 4.2.3.7
PISP: 4.2.3.8

Related CSRs: 1.11.5, 2.2.28, 5.1.3, 5.4.4, 5.4.5, 5.9.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Agreements should be such that the services to be provided in an emergency are clearly defined and understood by all parties concerned. Security and protection of information should be addressed in these agreements.

Protocols: 1. Examine organizational records or documents to determine if alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.
2. Examine alternate telecommunication service agreements to determine if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate processing site and telecommunications service controls are implemented.
4. Examine the alternate processing site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.
5. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates alternate processing site agreements on an ongoing basis.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews primary and alternate telecommunications service agreements on an ongoing basis.
7. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate processing sites and telecommunications services controls are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine the contingency plan to determine if the plan identifies the primary processing site hazards.
9. Examine the alternate processing site to determine if the site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.
10. Examine the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.
11. Examine alternate processing site agreements to determine if the agreements contain priority of service provisions in accordance with the organization's availability requirements.
12. Examine primary and alternate telecommunication service agreements to determine if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan.
13. Examine primary and alternate telecommunications service agreements and interview appropriate telecommunications service providers to determine if alternate and primary telecommunications services share a single point of failure.
14. Examine the alternate telecommunication service provider's site to determine if the site is sufficiently separated from the primary telecommunication service provider's site so as not to be susceptible to the same hazards identified at the primary site.
15. Examine the contingency plans from the primary and alternate telecommunication service providers to determine if the contingency plans are adequate.
16. Examine alternate processing site agreements to determine if the agreements specify the requirements needed to support the minimum required operational capability of the organization.
17. Test selected components of the information system at the alternate processing site to determine if the site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.

5.10.2 Arrangements are planned for travel and lodging of necessary disaster recovery personnel, if needed.

References:
CMS: Directed
FISCAM: TSC-3.2.3

Related CSRs: 5.2.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Disaster Recovery arrangements/plans should address persons that may need to come from distant locations as well as those that are local but who may need to stay at or near the data recovery site.

Protocols: 1. Verify by inspection that the required arrangements have been planned.

Category: ***Service Continuity***

General Requirement

Control Technique

5.10 Arrangements shall be made for alternate data processing and telecommunications facilities.

5.10.3 The backup storage and alternate processing sites are configured to facilitate timely and effective recovery operations. Capacity planning is conducted at alternate processing sites so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations. Potential accessibility problems to the sites in the event of an area-wide disruption or disaster are identified, and explicit mitigation actions are documented.

References:

ARS: CP-6.2
ARS: CP-6.3
ARS: CP-7.2
NIST 800-53: CP-2
NIST 800-53: CP-6
NIST 800-53: CP-7
PISP: 4.2.3.6
PISP: 4.2.3.7

Related CSRs: 5.4.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The alternate sites should be configured to allow for a timely recovery process. They should be geographically separated so as not to be susceptible to the same type of disruption or disaster.

Protocols: 1. Examine organizational records or documents to determine if alternate storage site agreements are currently in place to permit storage of information system backup information.
2. Examine organizational records or documents to determine if alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate storage and alternate processing site controls are implemented.
4. Examine the alternate storage site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information.
5. Examine the alternate processing site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.
6. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews and updates alternate storage and alternate processing site agreements on an ongoing basis.
7. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate storage and alternate processing site controls are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine the contingency plan to determine if the plan identifies the primary storage and alternate processing site hazards.
9. Examine the alternate storage and alternate processing sites to determine if the site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.
10. Examine the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.
11. Examine the alternate storage site agreement to determine if the agreement specifies requirements to facilitate timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives).
12. Test the alternate storage site operations to determine if the site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreement.
13. Examine alternate processing site agreements to determine if the agreements contain priority of service provisions in accordance with the organization's availability requirements.
14. Examine alternate processing site agreements to determine if the agreements specify the requirements needed to support the minimum required operational capability of the organization.
15. Examine the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.
16. Test selected components of the information system at the alternate processing site to determine if the site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.

5.10 Arrangements shall be made for alternate data processing and telecommunications facilities.

5.10.4 Alternate telecommunication services have been arranged. Alternate telecommunication providers do not share a single point of failure with primary telecommunications services, are sufficiently separated from the primary telecommunications services to prevent susceptibility to the same hazards, and have adequate Contingency Plans.

References:
ARS: CP-8.0
ARS: CP-8.1
ARS: CP-8.2
ARS: CP-8.3
ARS: CP-8.4
FISCAM: TSC-3.2.2
NIST 800-53: CP-8
PISP: 4.2.3.8

Related CSRs: 1.11.5, 5.7.5, 5.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A careful analysis should be made of all telecommunications utilized in normal times, and the links necessary to support critical functions identified.

Protocols: 1. Examine alternate telecommunication service agreements to determine if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the telecommunications services control is implemented.
3. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently reviews primary and alternate telecommunications service agreements on an ongoing basis.
4. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the telecommunications services control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Examine primary and alternate telecommunication service agreements to determine if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan.
6. Examine primary and alternate telecommunications service agreements and interview appropriate telecommunications service providers to determine if alternate and primary telecommunications services share a single point of failure.
7. Examine the alternate telecommunication service provider's site to determine if the site is sufficiently separated from the primary telecommunication service provider's site so as not to be susceptible to the same hazards identified at the primary site.
8. Examine the contingency plans from the primary and alternate telecommunication service providers to determine if the contingency plans are adequate.

5.11 A Contingency Plan shall exist for any standalone computer workstations that specifies where backup data, software, and current operating procedures are stored.

5.11.1 A Contingency Plan is available for each standalone computer workstation that specifies where backup data and software are stored. A single plan can cover more than one workstation.

References:
CMS: Directed

Related CSRs: 1.13.1, 1.13.5, 2.2.19, 5.4.1, 5.4.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Standalone workstations must be protected and contingency plans made for backup of their resident software and data.

Protocols: 1. Review documentation confirming that the specified plan is available for each standalone workstation.
2. Review the required contingency plan(s) to confirm inclusion of the specification of storage location(s) for backup data and software.

5.11.2 Standalone computer workstation backup data, software, and current operating procedures are stored in accordance with the Contingency Plan.

References:
CMS: Directed

Related CSRs: 5.2.8, 5.4.4, 5.4.5, 5.9.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is suggested that this back-up information be stored at a location different from the workstations.

Protocols: 1. Through inspection for a sample of standalone workstations, establish that the specified storage criteria are met.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

5.12 Detection of malicious software shall be performed.

5.12.1 The CMS Business Partner uses specialized software to accomplish identification, detection, protection, and elimination of malicious software, including malicious code, spam, and spyware. The software is managed centrally and automatically updated with the latest virus definitions and protection mechanisms whenever new releases are available.

References:
ARS: SI-3.1
ARS: SI-8.1
ARS: SI-8.2
FISCAM: TCC-1.3.2
HIPAA: 164.308(a)(5)(ii)(B)
NIST 800-53: SI-3
NIST 800-53: SI-8
PISP: 4.2.6.3
PISP: 4.2.6.8

Related CSRs: 1.1.1, 1.9.4, 1.13.8, 1.13.9, 2.2.24, 5.9.10, 10.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This special software should be approved and tested by knowledgeable persons before being installed.

Protocols: 1. Examine organizational records or documents to determine if the organization employs malicious code and spam protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).
2. Interview selected organizational personnel with system and information integrity responsibilities and examine malicious code protection mechanisms to determine if the mechanisms detect and eradicate malicious code transported: (i) by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes, or compact discs), or other common means; or (ii) by exploiting information system vulnerabilities.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software).
4. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization updates malicious code and spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the malicious code and spam protection controls are implemented.
7. Examine malicious code protection mechanisms to determine if the mechanisms are: (i) appropriately updated to include the latest malicious code definitions; (ii) configured to perform periodic scans of the information system as well as real-time scans of each file as it is downloaded, opened, or executed; and (iii) configured to disinfect and quarantine infected files.
8. Examine electronic mail clients and servers to determine if the clients and servers are configured to block attachments with file extensions associated with malicious code (e.g., .pifi .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe).
9. Examine the information system 's spam protection mechanism(s) by scanning critical information system entry points for the presence of spam.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently applies malicious code and spam protection measures within the information system on an ongoing basis.
11. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the malicious code and protection controls are documented and the resulting information used to actively improve the control on a continuous basis.
12. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization centrally manages malicious code protection mechanisms employed in organizational information systems.
13. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs a centralized management architecture to manage spam protection mechanisms for the information system.
14. Examine the information system configuration to determine if the malicious code protection mechanisms are configured to download and install updates automatically directly from the vendor or some other trusted source.
15. Examine spam protection mechanisms to determine if the mechanisms are configured to download and install updates automatically from the vendor or some other trusted source.

5.12 Detection of malicious software shall be performed.

5.12.2 Malicious code protection is implemented at information system entry points, including firewalls, e-mail servers, remote access servers, workstations, servers, and mobile computing devices. Automated mechanisms are employed to detect and eradicate malicious code transported by e-mail, e-mail attachments, and removable media.

References:
ARS: SI-3.0
NIST 800-53: SI-3
PISP: 4.2.6.3

Related CSRs: 1.9.4, 1.13.9, 10.2.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This special software should be approved and tested by knowledgeable persons before being installed.

Protocols:
1. Examine organizational records or documents to determine if the organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).
2. Interview selected organizational personnel with system and information integrity responsibilities and examine malicious code protection mechanisms to determine if the mechanisms detect and eradicate malicious code transported: (i) by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes, or compact discs), or other common means; or (ii) by exploiting information system vulnerabilities.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software).
4. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the malicious code protection control is implemented.
6. Examine malicious code protection mechanisms to determine if the mechanisms are: (i) appropriately updated to include the latest malicious code definitions; (ii) configured to perform periodic scans of the information system as well as real-time scans of each file as it is downloaded, opened, or executed; and (iii) configured to disinfect and quarantine infected files.
7. Examine electronic mail clients and servers to determine if the clients and servers are configured to block attachments with file extensions associated with malicious code (e.g., .pifi .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe).
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently applies malicious code protection measures within the information system on an ongoing basis.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the malicious code protection control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization centrally manages malicious code protection mechanisms employed in organizational information systems.
11. Examine the information system configuration to determine if the malicious code protection mechanisms are configured to download and install updates automatically directly from the vendor or some other trusted source.

6. Application Software Development and Change Control

6.1 Emergency changes to application software shall be promptly tested and approved.

6.1.1 Emergency changes are documented and approved by appropriate operations management, formally reported to appropriate computer operations management for follow-up, and approved after the fact by appropriate programming and user management.

References:
FISCAM: TCC-2.2.1
FISCAM: TCC-2.2.2

Related CSRs: 1.9.3, 2.4.1, 2.4.2, 5.6.3, 6.3.9, 6.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that the procedures for making emergency software changes are current and that emergency software changes are subsequently tested.

Protocols:
1. Review test plans and reports for the emergency changes.
2. For a sample of emergency changes, observe the required documentation and approval steps.
3. Interview the operations supervisor, computer operations management, programming supervisors, and user management.
4. Review the documented procedure required to process emergency changes.
5. Review the documentation of emergency change procedures.

6.2 Use of public domain and personal software shall be restricted.

6.2.1 Clear policies restricting the use of personal and public domain software have been developed and are enforced. Business rules and technical controls enforce the documented authorizations and prohibitions. Controls also prohibit the installation of any software by individuals other than by authorized information system or security personnel, unless authorized, in writing, by the SSO.

References:
ARS: SA-7.CMS-1
FISCAM: TCC-1.3.1
NIST 800-53: SA-7
PISP: 4.1.3.7

Related CSRs: 1.13.2, 1.13.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It may be necessary to periodically randomly inspect disk drives and servers to ensure that only approved personal or public domain software is resident.

Protocols: 1. Examine organizational documents or records to determine if the organization enforces explicit rules regarding the downloading and installation of software by users.
2. Examine organizational documents or records to determine if the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
3. Examine firewall logs for indications that prohibited software is operational within the information system. (Note: applications tend to communicate on known ports and/or have signature traffic patterns and common packets.)
4. Test the enforcement of rules for user installed software on the information system by attempting to download and install (from an account with user privileges) software that is strictly prohibited; compare the results with a similar test conducted on an account with administrative privileges; determine which account rights violated the rules for user installed software.
5. Test network traffic on the information system to determine if prohibited software is installed and operational by utilizing a network packet analyzer. (Note: Applications tend to communicate on known ports and/or have signature traffic patterns and common packets.)
6. Test the information system for prohibited software by utilizing a scanner which detects and reports the names of installed software; compare the results against the approved software applications list.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user installed software control is implemented.
8. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently enforces rules for the downloading and installation of software by users on an ongoing basis.
9. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user installed software control are documented and the resulting information used to actively improve the control on a continuous basis.

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.1 If new information systems are designed and implemented, the security engineering principles detailed in NIST SP 800-27 Rev. A are used. A configuration management plan that describes change control mechanisms, tracks security flaws, and defines change authorization requirements for the system is developed and implemented during system development.

References:
ARS: SA-10
ARS: SA-8.0
NIST 800-53: SA-10
NIST 800-53: SA-8
PISP: 4.1.3.10
PISP: 4.1.3.8

Related CSRs: 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that address these control objectives.

Protocols: 1. Examine organizational records or documents to determine if the organization considers security design principles in the development and implementation of the information system consistent with NIST SP 800-27.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security design principles control is implemented.
3. Examine the information system developer configuration management plan to determine if the developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and the plan implementation.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the developer configuration management control is implemented.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently applies security design principles in the development and implementation of organizational information systems on an ongoing basis.
6. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the information system developer consistently manages the information system configuration on an ongoing basis.
7. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security design principles control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the developer configuration management control are documented and the resulting information used to actively improve the control on a continuous basis.

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.2 A system development life cycle (SDLC) methodology has been developed that: (1) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (2) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; (3) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements; (4) complies with the information security steps of IEEE 12207.0 standard for SDLC as defined by CMS and/or the CMS Framework.

References:
ARS: SA-3.CMS-1
FISCAM: TCC-1.1.1
NIST 800-53: SA-3
PISP: 4.1.3.3

Related CSRs: 1.12.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that a current SDLC methodology exists, addresses security has been reviewed, and is being followed.

Protocols: 1. Examine organizational records or documents to determine if the organization manages the information system using a system development life cycle methodology that includes information security considerations.
2. Examine organizational records or documents to determine if the system development life cycle is consistent with NIST SP 800-64.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the life cycle support control is implemented.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently incorporates security considerations into the system development life cycle on an ongoing basis.
5. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the life cycle support control are documented and the resulting information used to actively improve the control on a continuous basis.

6.3.3 Security policy assigns responsibility to Application System Managers for ensuring that appropriate administrative, physical and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.

References:
CMS: Directed
HIPAA: 164.310(a)(1)

Related CSRs: 1.5.2, 1.5.5, 1.9.9, 5.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Tests should be performed and test reports should be reviewed to ensure that safeguards that protect software from unauthorized modification have been tested.`

Protocols: 1. Interview system programmers and administrators.
2. Review the documented policy to ensure that the required responsibilities are assigned.
3. Interview the application system managers.

6.3.4 Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.

References:
FISCAM: TCC-1.1.2

Related CSRs: 6.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Training plans and materials should exist for training in SDLC methodology.

Protocols: 1. Examine training plans and records.
2. Interview the programming staff and the software staff.
3. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current.

6.3.5 Changes to detailed system specifications are prepared by the programmer and reviewed by the appropriate supervisor or manager.

References:
FISCAM: TCC-2.1.2

Related CSRs: 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Specification changes are very important and can have far reaching effects. The requests for these should be carefully reviewed and approved by knowledgeable persons.

Protocols: 1. Review documented changes to system specifications.
2. Interview the programming supervisor.

6.3.6 Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.

References:
FISCAM: TCC-2.1.3

Related CSRs: 2.11.1, 3.4.1, 3.5.5, 6.1.1, 6.7.1, 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be documentation that provides a logical trace from initial requirements and specifications through to finished tested code, with no gaps in the trace path.

Protocols: 1. Review documented software changes to verify the tracing process.
2. Interview the software programming supervisor.

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.7 Test plan standards have been developed and are followed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).

References: FISCAM: TCC-2.1.1

Related CSRs: 1.4.3, 2.5.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good practice is to have independent tests performed.

Protocols:
1. Ensure through observation or interviews that during testing persons/groups fulfilled their responsibilities.
2. Interview department supervisors to verify their compliance with test plan standards.
3. Review test plan standards, and confirm that they follow all levels of testing and responsibilities.

6.3.8 Test plans are documented and approved that define responsibilities for each party involved.

References: FISCAM: TCC-2.1.4

Related CSRs: 2.5.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Persons involved in testing may include system analysts, programmers, quality assurance analysts, data base managers, security analyst, network analyst, software library control staff, users, system administrators, and test planners.

Protocols:
1. Interview test manager, and others as deemed necessary.
2. Verify that test plans are documented and approved, and define the required responsibilities.
3. Interview the system manager.

6.3.9 Unit, integration and system testing are performed and approved in accordance with the test plan. A sufficient range of valid and invalid conditions is applied.

References: FISCAM: TCC-2.1.5

Related CSRs: 2.5.6, 2.5.7, 3.5.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The test plan should be carefully reviewed to ensure that all necessary levels of testing are described and that test conditions are clearly defined. Test standards should be available.

Protocols:
1. Review test plan to ensure that it addresses test levels and conditions.
2. For the software change request selected: (1) Compare test documentation with related test plans; (2) Analyze test failures to determine if they indicate ineffective software testing.

6.3.10 A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. CMS sensitive data is not used in a developer or test environment.

References: FISCAM: TCC-2.1.6
FISCAM: TCC-2.1.7

Related CSRs: 1.9.4, 2.5.6, 2.5.7, 3.5.1, 4.7.5, 5.9.4, 6.4.1, 9.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: CMS sensitive data shall not be used in a developer or test environment. Tests should be conducted in an environment that simulates the conditions that are likely to be encountered when the changed software is implemented. A set of test transactions and data should be developed that contains examples of the various types of situations and information that the changed program will have to handle, including invalid transactions or conditions to make certain the software recognizes these transactions and reacts appropriately. In addition, the system's ability to process the anticipated volume of transactions within expected time frames should be tested.

Protocols:
1. Interview test programmers.
2. Verify that test data will meet all processing criteria.
3. Interview the system manager.
4. Confirm the restrictions in the use of live data.

6.3.11 Test results are reviewed and documented.

References: FISCAM: TCC-2.1.8

Related CSRs: 2.5.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: All test data, transactions, and results should be saved and documented. This will facilitate future testing of other modifications and allow a reconstruction if future events necessitate a revisit of the actual tests and results.

Protocols:
1. Interview the system manager.
2. Verify that test results are reviewed and documented.

6.3.12 Program changes are controlled as they progress through testing and are moved into production only upon documented approval from users and system development management.

References: FISCAM: TCC-2.1.9

Related CSRs: 3.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Persons that understand the changes made to software and the test results of those changes should approve moving the software from development into production.

Protocols:
1. Interview system development management.
2. Verify the documented approval of program changes before production implementation.
3. Interview user management.

Category: ***Application Software Development and Change Control***

General Requirement

Control Technique

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.13 Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented, or when system security controls are added or modified.

References:
FISCAM: TCC-2.1.10

Related CSRs: 1.8.3, 1.9.3, 1.9.4, 2.5.1, 2.5.6, 3.4.3, 3.4.5, 4.1.5, 5.4.3, 5.8.1, 5.9.4, 6.5.2, 10.7.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Documentation used by hardware, software, operations, and systems persons should reflect the latest system and software environment.

Protocols:
1. Interview the document control person (librarian).
2. Interview the system manager.
3. Review documentation of all required departments for prompt and accurate updating.

6.3.14 Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.

References:
FISCAM: TCC-2.1.11

Related CSRs: 3.1.2, 3.1.3, 3.3.3, 3.4.1, 4.4.1, 7.3.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Access controls and change controls should be periodically reviewed and/or tested to ensure their proper function.

Protocols:
1. Interview the system programmers and/or system administrator.
2. Interview data center management and/or the security administrator.
3. Determine when the last production program change was reviewed, and how often.

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.15 The flaw remediation process (e.g., hotfixes, patches, service packs) is managed centrally and updates (including virus definitions) are installed automatically. Automated mechanisms are employed periodically to determine the state of information system components with regard to flaw remediation.

Related CSRs: 1.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:
ARS: SI-2.0
ARS: SI-2.1
ARS: SI-2.2
ARS: SI-3.2
NIST 800-53: SI-2
NIST 800-53: SI-3
PISP: 4.2.6.2
PISP: 4.2.6.3

Guidance: It is important that there be expeditious installation of service packs, patches, and virus definitions while managing proper configuration management controls centrally.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization identifies recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the information system.
2. Examine organizational records or documents to determine if the organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).
3. Examine organizational records or documents to determine if the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures.
4. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures.
5. Examine organizational records or documents to determine if the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the flaw remediation control is implemented.
7. Examine organizational records or documents to determine if the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.
8. Test the information system with automated security tools to determine the effectiveness of the organization's flaw remediation capabilities.
9. Examine organizational records or documents containing a listing/log of recent security flaw remediation actions performed on the information system to determine if the system is appropriately modified to reflect the required flaw remediation.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently applies flaw remediation efforts within the information system on an ongoing basis.
11. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the flaw remediation control are documented and the resulting information used to actively improve the control on a continuous basis.
12. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization centrally manages the flaw remediation process for the information system.
13. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs a centralized patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches.
14. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization installs information system software updates automatically.
15. Examine the application that performs automatic updates to the information system software (or the documentation for the application) to determine how frequently automatic updates occur.
16. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to determine the security posture of information systems with respect to remediation of identified flaws.

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.16 Immediate (as required functionality allows) installation of vendor-supplied service packs, hot fixes, security patches, and virus definitions is enforced. Vendor-supplied security patches are obtained, analyzed for security and functionality in a test bed environment, and implemented on production equipment within 72 hours, or sufficient workaround procedures are implemented protect system assets.

References:
ARS: MA-2.0
ARS: SI-2.0
NIST 800-53: MA-2
NIST 800-53: SI-2
PISP: 4.2.5.2
PISP: 4.2.6.2

Related CSRs: 1.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is important that there be expeditious installation of service packs, patches, and virus definitions while maintaining proper controls configuration management and testing procedures.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization identifies recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the information system.
2. Examine organizational records or documents to determine if the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures.
4. Examine organizational records or documents to determine if the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the flaw remediation control is implemented.
6. Examine organizational records or documents to determine if the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.
7. Test the information system with automated security tools to determine the effectiveness of the organization's flaw remediation capabilities.
8. Examine organizational records or documents containing a listing/log of recent security flaw remediation actions performed on the information system to determine if the system is appropriately modified to reflect the required flaw remediation.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently applies flaw remediation efforts within the information system on an ongoing basis.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the flaw remediation control are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization centrally manages the flaw remediation process for the information system.
12. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs a centralized patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches.
13. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization installs information system software updates automatically.
14. Examine the application that performs automatic updates to the information system software (or the documentation for the application) to determine how frequently automatic updates occur.
15. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to determine the security posture of information systems with respect to remediation of identified flaws.

6.4 Access to program libraries shall be restricted.

6.4.1 Separate libraries are maintained for program development and maintenance, testing, and production programs. Production source code is maintained in a separate archive library.

References:
FISCAM: TCC-3.2.1
FISCAM: TCC-3.2.2

Related CSRs: 2.2.22, 2.10.2, 6.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The separate libraries should each have their own set of access controls so that, for example, testers cannot access production code. The separate archive library should be protected from unauthorized access by software or physical controls.

Protocols: 1. Monitor libraries in use.
2. Interview library control personnel.
3. Verify that source code exists for a selection of production load modules by: (1) comparing compile dates; (2) recompiling the source modules; and (3) comparing the resulting module size to production load module size.

6.4 Access to program libraries shall be restricted.

6.4.2 Access to all programs, including production code, source code, and extra program copies, is protected by access control software and operating system features.

References:
FISCAM: TCC-3.2.3
HIPAA: 164.312(a)(1)
HIPAA: 164.312(e)(1)

Related CSRs: 1.4.3, 1.5.5, 2.8.3, 2.10.2, 3.3.1, 5.2.8, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Separate software libraries should be established and only the library control group should be allowed move programs between libraries. Programmers should only have access to the programs they are assigned.

Protocols: 1. Determine if the access controls are implemented and working.
2. For critical software production programs, determine whether access control software rules are clearly defined.

6.4.3 All deposits and withdrawals of program tapes and other storage media to/from the library are authorized and recorded.

References:
FISCAM: TCC-3.2.4

Related CSRs: 1.3.10, 2.2.13, 2.2.17, 2.8.3, 2.13.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: The library record should be protected from exposure to unauthorized changes or release.

Protocols: 1. Select other storage media from the record and verify the existence of the media either in the library or with the individual responsible for withdrawing the media.
2. Select a few program tapes from the record and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tape.

6.5 Distribution and implementation of new or revised software shall be controlled.

6.5.1 Standardized procedures are implemented to distribute new software for implementation.

References:
FISCAM: TCC-2.3.1

Related CSRs: 1.9.4, 2.11.1, 3.1.3, 3.4.1, 3.4.4, 10.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Software should be distributed allowing enough time at the site for installation, testing, and migration to production.

Protocols: 1. Examine procedures for distributing new software.

6.5.2 The distribution and implementation of new or revised software is documented and reviewed. Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.

References:
FISCAM: TCC-2.3.2

Related CSRs: 1.9.9, 3.5.1, 6.3.13

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The implementation order should leave no doubt as to when the new software should start to be used for production.

Protocols: 1. Check the distribution and implementation orders for a sample of changes.
2. Examine distribution and implementation procedures for distributing new or revised software.

6.6 Programs shall be automatically labeled and inventoried.

6.6.1 Library management software is used to produce audit records of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.

References:
FISCAM: TCC-3.1

Related CSRs: 1.3.11, 2.11.1, 3.4.1, 3.5.1, 3.5.5, 5.9.4, 6.1.1, 6.8.1, 10.7.2, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Software controls should be easily monitored and audited. Library management of software helps ensure that differing versions are not accidentally misidentified.

Protocols: 1. Review software change control policies and procedures.
2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures.
3. Interview personnel responsible for library control.

6.7 Authorizations for software modifications shall be documented and maintained.

6.7.1 Software change request forms are used to document software modification requests and related approvals.

References:
FISCAM: TCC-1.2.1

Related CSRs: 6.3.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The forms should be designed such that they help ensure that change requests are clearly communicated. The authorization form may be maintained as paper or softcopy format.

Protocols: 1. Examine a selection of software change or modification request forms for approvals.

6.7 Authorizations for software modifications shall be documented and maintained.

6.7.2 Change requests are approved by both system users and data processing staff.

References:
FISCAM: TCC-1.2.2

Related CSRs: 3.4.1, 3.5.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good practice is to convene the change-control board to assure all appropriate personnel provide input and approval for software modifications and document the approval of the proposed changes.

Protocols: 1. Determine if the change requests for past changes have been approved.
2. Identify recent software modifications and determine whether change request forms were used.
3. Interview software development staff.

6.8 Movement of programs and data among libraries shall be controlled.

6.8.1 A group independent of users and programmers controls movement of programs and data among libraries.

References:
FISCAM: TCC-3.3.1

Related CSRs: 2.10.2, 3.4.2, 6.3.4, 6.3.7, 6.4.1, 6.4.3, 6.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Prior to moving software from a test to production environment, an independent review of the changes developed and tested should be made.

Protocols: 1. Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.

6.8.2 Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.

References:
FISCAM: TCC-3.3.2

Related CSRs: 3.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An independent library control group should make the image comparisons.

Protocols: 1. Examine some of the images of stored code that has been changed.
2. Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared.

7. Application System Authorization Controls

7.1 Source documents shall be controlled and shall require authorizing signatures.

7.1.1 Source documents (e.g., checks, claims forms, etc.) are pre-numbered to maintain control over the documents. Key source documents require authorizing signatures.

References:
FISCAM: TAN-1.1.2
FISCAM: TAN-1.1.3

Related CSRs: 2.6.1, 2.13.1

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents. Pre-numbered documents help/prevents missing or lost documents.

Protocols: 1. Review documentation identifying "key source documents".
2. Review the documented procedure for recording and tracking of document numbers.
3. Confirm that documents contain authorized signatures.
4. Inspect audit data confirming that the required process is consistently used.

7.1.2 For batch application systems, a batch control sheet is prepared for a group of source documents and includes: date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

References:
FISCAM: TAN-1.1.4

Related CSRs: 2.10.2

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: A preformatted batch control sheet will simplify the tracking process for batch application systems or interactive systems with batching capabilities.

Protocols: 1. Check a sample of batch control sheets to ensure the inclusion of the Control Technique elements.
2. Review the documented procedure for batch control sheet preparation.

7.1.3 Access to blank documents (e.g., checks, claims forms, etc.) is restricted to authorized personnel.

References:
FISCAM: TAN-1.1.1

Related CSRs: 1.1.5

Applicability: ABMAC, COB, DMEMAC, PartA, PartB, PSC

Guidance: It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents.

Protocols: 1. Review documented procedure containing authorized names and control of access.
2. Inspect blank document storage access controls for conformance to documented policy.
3. Interview a sample of personnel to confirm use of documented handling procedures.

7.2 Master files shall be used to identify unauthorized transactions.

7.2.1 Before transactions are processed, they are verified using master files of approved vendors, employees, etc., as appropriate for the application.

References:
FISCAM: TAN-3.1.1

Related CSRs: 2.10.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is a good practice to verify the transaction is applicable before any transactions are processed. For example, a procurement system requires approved vendors prior to processing of transactions.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

7.2.2 Master files and program code that does the verification are protected from unauthorized modification.

References:
FISCAM: TAN-3.1.2

Related CSRs: 2.6.1, 2.13.1, 5.2.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The organization should maintain an application protection policy regarding the protection and modification of application master files and program code. A recommendation could be to include the policy in the application change management process or part of the organization's security profile.

Protocols: 1. Review documentation of software controls used in providing the required protection.
2. Inspect audit data confirming that the required process is consistently used.
3. Review the documented procedure covering the protection of master files and program code.
4. Identify and observe the procedures employed that protect master files and program code.

7.3 Data entry workstations shall be secured and restricted to authorized users.

7.3.1 Data entry workstations are connected to the system only during specific periods of the day, which corresponds with the business hours of the data entry personnel.

References:
FISCAM: TAN-2.1.5

Related CSRs: 1.13.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review the workstation policy/guidelines.

Protocols: 1. Observe workstation use.
2. Review documented procedure for workstation use.
3. Inspect audit data confirming that the required process is consistently used.

7.3.2 Data entry workstations are located in physically secure environments and monitors are positioned to eliminate viewing by unauthorized persons.

References:
ARS: PE-5.0
FISCAM: TAN-2.1.1
NIST 800-53: PE-5
PISP: 4.2.2.5

Related CSRs: 2.2.6, 2.2.19

Applicability: ABMAC, COB, DMEMAC, PartA, PartB, PSC, SS

Guidance: Workstations processing or connected to systems processing sensitive data are located in physically secure areas.

Protocols: 1. Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for display medium control is implemented.
3. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently controls physical access to system devices that display information on an ongoing basis.
4. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for display medium control are documented and the resulting information used to actively improve the control on a continuous basis.

7.3.3 Each operator is required to use a unique password and identification code before being granted access to the system.

References:
FISCAM: TAN-2.1.4

Related CSRs: 2.9.3, 2.9.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses, including the use of password and identification control.

Protocols: 1. Observe a sample of data entry login.
2. Review documented log in procedure.
3. Interview a sample of management and data entry personnel to confirm consistent use of the documented procedure. Confirm that there is no sharing of passwords or identification codes.

7.3 Data entry workstations shall be secured and restricted to authorized users.

7.3.4 All transactions are recorded as entered, along with the UserID of the person entering the data.

References:
FISCAM: TAN-2.1.9

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 4.2.2, 8.1.1, 8.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This is a function of the audit process. It is a good practice to manually review the audit records to validate that the data entry process is correct.

Protocols: 1. Review the documented procedure prescribing transaction recording.
2. Observe the processing of sample transactions, to ascertain that they are being recorded correctly.

7.3.5 When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.

References:
FISCAM: TAN-2.1.2

Related CSRs: 1.13.1, 2.2.19

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Review the workstation policy/guidelines.

Protocols: 1. Observe physical area during non-business hours.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Inspect audit data confirming that the required process is consistently used.

7.3.6 Online access records are maintained by the system and reviewed regularly for unauthorized access attempts.

References:
FISCAM: TAN-2.1.8

Related CSRs: 2.6.1, 2.9.10, 2.13.1, 2.13.2, 4.2.2, 6.3.14, 8.1.1, 8.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This is a function of the audit process. It is a good practice to manually review the audit records to validate that the online access process is correct.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

7.4 Users shall be limited to a set of authorized transactions.

7.4.1 Authorization profiles for users or workstations limit what transactions personnel can enter.

References:
FISCAM: TAN-2.2.1
FISCAM: TAN-2.2.2

Related CSRs: 1.13.1, 2.9.4, 2.10.3, 2.10.4, 10.8.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The supervisors should address access limitations in the ACL. Review the application processing policy/guidelines.

Protocols: 1. Review documented procedure for data entry to confirm enforcement of the required limitation.
2. Review audit controls used to assure continued application of the required procedure.
3. For a sample of each type of restricted workstation, observe attempted entry of a prohibited transaction by a logged on user who has the user permissions required to enter the transaction.

7.5 Exceptions shall be reported to management for review and approval.

7.5.1 Exceptions, based on parameters established by management, are reported for their review and approval.

References:
FISCAM: TAN-3.2.1

Related CSRs: 1.13.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: An exception report lists items requiring review and approval. These items may be valid, but exceed parameters established by management. For, example, in a disbursement system, all disbursements exceeding $20,000 could be reported to management for their review and approval before the disbursements are released.

Protocols: 1. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.
2. Inspect audit data confirming that the required process is consistently used.

7.6 Independent reviews of data shall occur before entering the application system.

7.6.1 Procedures are implemented for a multilevel review of CMS sensitive input data before it is released for processing.

References:
ARS: SI-10.CMS-1
FISCAM: TAN-1.2.3
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 4.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: It is a good practice to validate the authorization list and to have a preformatted review list in place for processing CMS sensitive data.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

7.6.2 Data control unit personnel verify that source documents are properly prepared and authorized, and monitor data entry and processing of source documents.

References:
FISCAM: TAN-1.2.1
FISCAM: TAN-1.2.2

Related CSRs: 8.4.5, 8.5.1, 8.5.2

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: The data control unit is the quality assurance personnel group that validates the data on the source documents before the data is entered. Additionally, this group can monitor the data entry process for accuracy.

Protocols: 1. Observe data control unit personnel performing the verification process.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Interview management and data control unit personnel to confirm use of the process.
4. Inspect audit data confirming that the required process is consistently used.
5. Observe data entry and processing procedures.

8. Application System Completeness Controls

8.1 Computer sequence-checking shall be implemented.

8.1.1 Sequence checking is used to identify missing or duplicate transactions. Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.

References:
FISCAM: TCP-1.2.3
FISCAM: TCP-1.2.4

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 4.2.2, 7.3.4, 7.3.6, 8.2.1, 9.6.5

Applicability: COB, PSC, SS

Guidance: The possibility of alterations, missing transactions or duplicate transactions can occur if sequence numbers are not properly processed. If a sequence number is missing it may have been deleted or misplaced. The missing or duplicate data files should be investigated and corrective actions taken. An alteration to the data files should be investigated and needed corrective actions taken. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation so that timely action(s) can be taken.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review reports of missing or duplicate transactions.

8.1.2 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.

References:
FISCAM: TCP-1.2.1

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 4.2.2

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Serial numbers for source documents assist in the tracking of source documents. Additionally, the sequence of the serial numbers processed shows that a source document has not been inadvertently missed or an unauthorized transaction has been inserted into the process.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

8.1 Computer sequence-checking shall be implemented.

8.1.3 Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.

References: FISCAM: TCP-1.2.2

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 4.2.2 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This is a function of the processing application. The application developer or vendor should verify the existence of transaction serial numbers being assigned, and sequence number checking routines or modules included in the application.

Protocols: 1. Interview the system owner and determine what policies and corrective action are in place when a sequence number error occurs.
2. Verify, though documentation review, that the application contains automatic routines for checking sequence numbers and appropriate reports/alerts are generated when serial numbers are not processed in sequence or duplicated.
3. Inspect audit data confirming that the required process is consistently used.
4. Review the documented procedure that prescribes the assigning of unique sequence numbers.
5. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers.

8.2 Computer matching of transaction data shall be implemented.

8.2.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.

References: FISCAM: TCP-1.3.2

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 7.3.4, 7.3.6, 8.1.1, 9.6.5 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The possibility of an alteration to the data files should be investigated and needed corrective actions taken. For example, within the policy guidelines, actions should include notifying the resource owner of the violation.

Protocols: 1. Verify the application has an assigned system owner.
2. Verify the application has the ability to insert the preassigned source document numbers matched with the associated data.
3. Inspect audit data confirming that the required process is consistently used.
4. Review relevant policies and procedures for inclusion and directed use of the required process.

8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.

References: FISCAM: TCP-1.3.1

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 4.2.2, 9.3.4, 9.3.5 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The purpose of this CSR is to ensure that data input was completed thoroughly and nothing was duplicated or left out. The possibility of an alteration to the data files should be investigated and needed corrective actions taken. For example, within the policy guidelines, actions should include notifying the resource owner of the violation.

Protocols: 1. Verify that a system owner has been designated and when errors occur, that person is notified.
2. Inspect audit data confirming that the required process is consistently used.
3. Review the program specifications that describe the computer matching process.

8.2.3 For high-value, low-volume items, individual transactions or source documents are compared with a detailed listing of items processed by the computer.

References: FISCAM: TCP-1.4

Related CSRs: 2.1.5, 2.1.7, 2.1.11 Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This process is application dependent, but should be automated as much as possible. If an automated function is not available for the software, then consideration for developing such a process would improve the security of the application. High value items need special attention.

Protocols: 1. Verify that a staff person is assigned and responsible for verifying that high-value transaction data accurately reflects data from the source documentation.
2. Inspect audit data confirming that the required process is consistently used.
3. Inspect documentation identifying items designated as high-value, low volume.
4. Review the documented procedure that describes the comparison process.

8.3 Reconciliations shall show the completeness of the data processed for the total cycle.

8.3.1 Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.

References: FISCAM: TCP-2.2

Related CSRs: 2.1.5, 2.1.7, 2.1.11 Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This process is application dependent, but should be automated as much as possible.

Protocols: 1. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.
2. Review the documented procedure describing the reconciliation process.
3. Inspect audit data confirming that the required process is consistently used.

8.4 Reconciliations shall show the completeness of data processed at points in the processing cycle.

8.4.1 Record counts and control totals are established over time and entered with transaction data, and subsequently reconciled to determine the completeness of data entry.

References:
ARS: SI-10.CMS-1
FISCAM: TCP-2.1.1
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 2.1.5, 2.1.7, 2.1.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The application should be tracking each transaction and reconciling any differences with the data being entered. (commonly called "run-to-run control totals")

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., record counts, control totals, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

8.4.2 Trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed.

References:
ARS: SI-10.CMS-1
FISCAM: TCP-2.1.2
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 2.1.5, 2.1.7, 2.1.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Trailer labels may include any number of tracking or checking techniques. The Trailer labels verify the accuracy of the process, but not the data entry accuracy. If the data is entered correctly and the data is processed completely, then there should not be errors in the output.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., trailor labels, control records, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

8.4 Reconciliations shall show the completeness of data processed at points in the processing cycle.

8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.

References:
ARS: SI-10.CMS-1
FISCAM: TCP-2.1.3
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 2.1.5, 2.1.7, 2.1.11

Applicability: COB, CWF, DC, EDC, PSC, SS

Guidance: This process is largely application dependent, but should be automated as much as possible. If an automated function is not available for the software, then consideration for developing such a process would improve the security of the application.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., control totals, run-to-run totals, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

8.4.4 System interfaces require that the sending system's output control counts equal the receiving system's input counts.

References:
ARS: SI-10.CMS-1
FISCAM: TCP-2.1.4
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 2.1.5, 2.1.7, 2.1.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: As systems have become more integrated over the years, a file produced by one application may be used in another application. It is important to reconcile control information between the sending and receiving applications.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., output and input counts, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

8.4.5 A data processing control group receives and reviews control total reports and determines the completeness of processing.

References:
FISCAM: TCP-2.1.5

Related CSRs: 2.1.5, 2.1.7, 2.1.11, 7.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Performing the comparison of control numbers is commonly referred to as balancing, and should be done automatically by the computer, although some older systems may rely on manual balancing procedures. The control numbers for the balancing at key points should be documented, such as being printed on a control totals report, and should be reviewed by the data processing control group that monitors the completeness and accuracy of processing.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented procedure describing the data control group's function.

Category: ***Application System Completeness Controls***

General Requirement

Control Technique

8.5 Record counts and control totals shall be implemented on an IT System.

8.5.1 For on-line or real time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness of data entry and processing.

References:
ARS: SI-10.CMS-1
FISCAM: TCP-1.1.2
HSPD-7: G(24)
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 2.1.5, 2.1.7, 2.1.11, 7.6.2

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: This is part of the quality assurance process. Since the processing is on-line or real-time, the system can not be taken down for validation of processing. The only way to validate the processing accuracy is to take a snap shot or monitor the processing for accuracy by taking a sampling over a period of time.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., record counts, control totals, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

8.5.2 User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.

References:
ARS: SI-10.CMS-1
FISCAM: TCP-1.1.1
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 2.1.5, 2.1.7, 2.1.11, 7.6.2

Applicability: ABMAC, COB, DMEMAC, PartA, PartB, PSC

Guidance: In general, user-prepared totals established over source documents and data to be entered can be carried into and through processing. The computer can generate similar totals and track the data from one processing stage to the next and verify that the data was entered and processed as it should have been.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., record counts, control totals, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Application System Accuracy Controls***
General Requirement
Control Technique

9. Application System Accuracy Controls

9.1 Instances of erroneous data shall be reported back to the user departments for investigation and correction.

9.1.1 Error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error. Errors are corrected by the user originating the transaction.

References:
FISCAM: TAY-3.2.1
FISCAM: TAY-3.2.2

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.1, 4.1.4, 9.3.1, 9.3.2, 9.3.5, 9.6.5, 9.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach to tracking errors and developing procedures to minimize errors would be a detailed error list for managers and supervisors to track and expand corrective actions. Error messages should clearly indicate what the error is and what corrective action is necessary.
Some systems may use error reports to communicate to the user department the rejected transactions in need of correction. More modern systems will provide user departments access to a file containing erroneous transactions. Using a computer terminal or workstation, users can initiate corrective actions. The user responsible for originating the transaction should be responsible for correcting the error.

Protocols: 1. Review the documented error processing and correction procedures.
2. Review sample error reports/files, and confirm that error messages contain the information specified in the Control Techniques.
3. Interview a sample of supervisors and subordinate personnel to confirm that all specified reports and files have the required characteristics.
4. Inspect audit data confirming that the required process is consistently used.

9.1.2 All corrections are reviewed and approved by supervisors before the corrections are reentered. (Based on the Medicare operating environment, Business Partners may have other compensating controls in place.)

References:
FISCAM: TAY-3.2.3

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11

Applicability: ABMAC, COB, DMEMAC, PartA, PartB, PSC

Guidance: As part of the formal security program, policies should be in a procedures document with system security features for error-correction procedures included. All corrections should be reviewed and approved by supervisors before being reentered into the system, or released for processing if corrected from a computer terminal or workstation.

Protocols: 1. Interview a sample of supervisors and subordinate personnel to confirm use of the required process.
2. Review the documented error correction procedure for inclusion of the required process.
3. Inspect audit data confirming that the required process is consistently used.

9.2 Automated entry devices shall be used to increase data accuracy.

9.2.1 Effective use is made of automated entry devices to reduce the potential for data entry errors.

References:
FISCAM: TAY-1.4

Related CSRs: 2.2.3

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The use of automated entry devices (e.g., optical or magnetic ink character readers) can reduce data error rates, as well as speed the entry process. IRS' use of preprinted labels, showing the taxpayer's name, address, and social security number is such an example. This information can be entered without keying the data, which ensures a more accurate and faster process. A good approach validating compliance would be to document the security features of the system that spells out the characteristics of the automated data entry devices so that an audit of the procedures and devices can easily be evaluated.

Protocols: 1. Review the documentation explaining how the specified objective is met.

9.3 Rejected transactions shall be controlled with an automated error suspense file.

9.3.1 Rejected data are automatically written on an automated suspense file and held until corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error; (2) date and time the transaction was processed and the error identified; and (3) the identity of the user who originated the transaction.

References:
FISCAM: TAY-3.1.1

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 3.1.5, 4.1.1, 4.1.4, 9.1.1, 9.5.1, 9.6.7, 9.6.8, 9.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: As part of the formal security program, policies should be delineated in a procedures document with system security features for error-correction procedures included. A security audit review process should be documented and implemented.

Protocols: 1. Review the documented procedure for processing reject data to confirm inclusion of the specified features.
2. Inspect audit data confirming that the required process is consistently used.

9.3 Rejected transactions shall be controlled with an automated error suspense file.

9.3.2 A control group is responsible for controlling and monitoring rejected transactions.

References: FISCAM: TAY-3.1.3

Related CSRs: 9.1.1

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: A good approach would be to document the security features of the system that spells out system monitoring characteristics and the reasons for transaction rejections. Corrective action procedures should be documented and evaluated as well.

Protocols: 1. Interview a sample of the control group to confirm operational responsibilities match those documented.
2. Review the documented procedure describing the control group's responsibilities and duties.

9.3.3 The suspense file is purged of transactions as they are corrected. However, general controls effectively protect the suspense file from unauthorized access and modification.

References: FISCAM: TAY-3.1.4
FISCAM: TAY-3.1.6

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 2.8.4, 5.2.8

Applicability: COB, PSC, SS

Guidance: The suspense file should be purged of the related erroneous transaction as the correction is made. Record counts and control totals for the suspense file should be adjusted accordingly. Suspense files are normally created as the result of data needing to be input into the system or a correction to data errors.
General controls should protect the suspense file from unauthorized access and modification, in order for the auditor to be able to rely on this control technique to reduce audit risk. A good approach would be to document the security features of the system, spelling out system monitoring characteristics and the action taken when policies are not followed.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented procedure for the error correction process to confirm inclusion of the specified process.
3. Review the documentation describing how general controls provide the required protection of the suspense file.

9.3.4 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.

References: FISCAM: TAY-3.1.2

Related CSRs: 8.2.2

Applicability: ABMAC, COB, CWF, DMEMAC, PartA, PartB, PSC, SS

Guidance: Record counts and control totals should be developed automatically during processing of erroneous transactions to the suspense file and used in reconciling the transactions successfully processed. A control group should be responsible for controlling and monitoring the rejected transactions. The records count is a good management tool that assists in the administration of vital resources used to reconcile security transaction processing.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Observe the suspense file process to confirm that the documented procedure is followed.
3. Review the documented procedure for suspense file processing and transaction reconciliation.

9.3.5 The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected errors.

References: FISCAM: TAY-3.1.5

Related CSRs: 3.1.5, 8.2.2, 9.1.1, 9.5.1, 9.6.7, 9.6.8

Applicability: ABMAC, COB, DMEMAC, PartA, PartB, PSC

Guidance: Periodically, the suspense file should be analyzed to determine the extent and type of transaction errors being made, and the age of uncorrected transactions. This analysis may indicate a need for a system change or some specific training to reduce future data errors. The suspense file is a good management tool that assists in the administration of vital resources used to reconcile transaction processing.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented suspense file procedure for inclusion of the specified processes.

9.4 Source documents shall be designed to minimize errors.

9.4.1 The source document is well-designed to aid the preparer and facilitate data entry. Transaction type and date field codes are preprinted on the source document.

References: FISCAM: TAY-1.1.1
FISCAM: TAY-1.1.2

Related CSRs: 1.9.2, 9.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to have needed data entry information succinctly formatted to facilitate ease of data entry.

Protocols: 1. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.
2. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry".

9.5 Overriding or bypassing data validation and editing shall be restricted.

9.5.1 Overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically recorded by the application so that the action can be analyzed for appropriateness and correctness.

References:
FISCAM: TAY-2.3.1
FISCAM: TAY-2.3.2

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.1, 4.1.4, 9.3.1, 9.3.5, 9.7.1

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: As part of the formal security program, policies should be delineated in a procedures document with system security features for error-correction procedures included. A security audit review process should be documented and implemented.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls.

9.6 Output production and distribution shall be controlled.

9.6.1 Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design.

References:
FISCAM: TAY-4.1.1

Related CSRs: 1.4.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Security policies are distributed to all affected personnel to include system and application rules, rules to clearly delineate responsibility, and rules to describe expected behavior of all with access to the system.

Protocols: 1. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.
2. Review the documented procedure assigning responsibility for output production and distribution.

9.6.2 The computer system automatically checks the output message before displaying, writing, and printing to make sure the output has not reached the wrong workstation device. A connection must be established to a specific device (workstation, printer, etc.) and verified by the system before transmitting data.

References:
FISCAM: TAY-4.1.6

Related CSRs: 9.8.1, 9.8.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.

Protocols: 1. Review documentation describing how the required control is implemented.
2. Review documentation confirming use of the required process.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

9.6.3 Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.

References:
FISCAM: TAY-4.1.7

Related CSRs: 1.5.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The printed reports are good management tools to assist in the tracking of completed tasks.

Protocols: 1. Review the documented procedure describing the output process and supervisory review.
2. Inspect audit data confirming that the required process is consistently used.

9.6.4 The data processing control group, or some alternative, has a schedule by application that shows: (1) when outputs are completed; (2) when they need to be distributed; (3) who the recipients are; and (4) the copies needed. The group then reviews output products for general acceptability and reconciles control information to determine completeness of processing.

References:
FISCAM: TAY-4.1.2

Related CSRs: 1.5.2, 1.5.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted. The data control group becomes the baseline for that standard by which the output quality is measured.

Protocols: 1. Inspect audit data confirming that the required process is consistently used.
2. Inspect the required schedule to confirm inclusion of the required elements.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

9.6 Output production and distribution shall be controlled.

9.6.5 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message. They are also labeled (marked) externally with the appropriate security level classification and any distribution limitations or handling caveats of the information.

References:
ARS: AC-15
ARS: MP-3.0
FISCAM: TAY-4.1.3
NIST 800-53: AC-15
NIST 800-53: MP-3
PISP: 4.2.7.3
PISP: 4.3.2.15

Related CSRs: 8.1.1, 8.2.1, 9.1.1, 9.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The printed report name, time, and date are good management tools to assist in the tracking of completed tasks.

Protocols: 1. Examine information system output to determine if standard naming conventions are used to identify any special dissemination, handling, or distribution instructions.
2. Examine organizational records or documents to determine if the organization: (i) affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information; and (ii) exempts specific types of media or hardware components from labeling so long as they remain within a secure environment.
3. Examine the configuration of the information system to determine how the system automatically marks the output for any special disseminating, handling or distribution instructions.
4. Test the automated marking capability in the information system by executing processes to produce outputs to determine if the outputs are automatically marked using standard naming conventions and include any defined special dissemination, handling, or distribution instructions in accordance with the automated marking policy and procedures.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the automated marking control is implemented.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently implements automated marking of information system output on an ongoing basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the automated marking control are documented and the resulting information used to actively improve the control on a continuous basis.

9.6.6 Each output produced is recorded, manually if not automatically, including the recipient(s) who receive the output.

References:
ARS: AC-15
FISCAM: TAY-4.1.4
NIST 800-53: AC-15
PISP: 4.3.2.15

Related CSRs: 1.5.2, 3.2.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The output report record is a good management tool to assist in the tracking of completed tasks.

Protocols: 1. Examine information system output to determine if standard naming conventions are used to identify any special dissemination, handling, or distribution instructions.
2. Examine the configuration of the information system to determine how the system automatically marks the output for any special disseminating, handling or distribution instructions.
3. Test the automated marking capability in the information system by executing processes to produce outputs to determine if the outputs are automatically marked using standard naming conventions and include any defined special dissemination, handling, or distribution instructions in accordance with the automated marking policy and procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the automated marking control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently implements automated marking of information system output on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the automated marking control are documented and the resulting information used to actively improve the control on a continuous basis.

9.6.7 A control record of output product errors is maintained, including the corrective actions taken.

References:
FISCAM: TAY-4.1.8

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.1, 4.1.4, 9.3.1, 9.3.5, 9.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The control record, with the suspense file, provides statistics on corrective action required and actions taken. This assists management in the status and use of its personnel and equipment resource tracking. Additionally, product errors may effect the implementation of a change request with appropriate security issues that can be addressed.

Protocols: 1. Review the control record and confirm that it contains the required information.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

9.6 Output production and distribution shall be controlled.

9.6.8 Output from reruns is subjected to the same quality review as the original output.

References:
FISCAM: TAY-4.1.9

Related CSRs: 2.1.2, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.1, 4.1.4, 9.3.1, 9.3.5, 9.7.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

9.7 Reports showing the results of processing shall be reviewed by users.

9.7.1 Users review output reports for data accuracy, validity, and completeness. The reports include error reports, transaction reports, master record change reports, exception reports, and control totals balance reports.

References:
ARS: SI-10
FISCAM: TAY-4.2
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 3.1.5, 3.4.1, 9.1.1, 9.3.1, 9.5.1, 9.6.5, 9.6.7, 9.6.8

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

9.8 Programmed validation and edit checks shall identify erroneous data.

9.8.1 The following are protected from unauthorized modifications: (1) program code for data validation and editing and associated tables or files; (2) program code and criteria for test of critical calculations; and (3) exception criteria and the related program code. Programs perform limit and reasonableness checks on critical calculations.

References:
ARS: SI-7.0
FISCAM: TAY-2.1.4
FISCAM: TAY-2.2.1
FISCAM: TAY-2.2.2
NIST 800-53: SI-7
PISP: 4.2.6.7

Related CSRs: 3.4.1, 5.2.8, 9.6.2

Applicability: ABMAC, COB, DC, EDC, PartA, PSC, SS

Guidance: Before an auditor can rely on the entity's data validation and editing checks that are meant to reduce the audit risk, the auditor must determine the adequacy of the general controls over those checks. To be effective, the general controls should protect the program code and any related tables associated with the validation and edit routines from unauthorized changes.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs integrity verification software on the information system to look for evidence of information tampering, errors, and omissions.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes).
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs tools to automatically monitor the integrity of the information system and the applications the system hosts.
4. Examine information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system detects and protects against unauthorized changes to software and information on an ongoing basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software and information integrity control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Application System Accuracy Controls***

General Requirement

Control Technique

9.8 Programmed validation and edit checks shall identify erroneous data.

9.8.2 Programmed validation and edits include checks for: (1) reasonableness; (2) dependency; (3) existence; (4) mathematical accuracy; (5) range; (6) check digit; (7) document reconciliation; and (8) relationship or prior data matching.

References:
ARS: SI-10
FISCAM: TAY-2.1.1
NIST 800-53: SI-10
PISP: 4.2.6.10

Related CSRs: 3.4.1, 9.6.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Programmed validation and edit checks are, for the most part, the most critical and comprehensive way to ensure that the initial recording of data into the system is accurate. For example, programmed validation and edit checks can effectively start as the data are being keyed in at a computer workstation using preformatted computer screens.

Protocols: 1. Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.
2. Examine the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.
3. Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.

9.8.3 Validation and editing are performed at the computer workstation during data entry or as early as possible in the data flow and before updating the master files. All data fields are checked for errors before rejecting a transaction.

References:
FISCAM: TAY-2.1.2
FISCAM: TAY-2.1.3

Related CSRs: 3.4.1

Applicability: ABMAC, COB, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Validation of the accuracy of data assists in the integrity of the data being processed.

Protocols: 1. Observe the validation and edit process.
2. Inspect audit data confirming that the required process is consistently used.
3. Review the documented procedure describing the specified validation and editing process.

9.8.4 Off-the-shelf integrity mechanisms such as parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes are used to detect and protect against information tampering, errors, omissions and unauthorized changes to software; and tools are used to automatically monitor the integrity of the information system and the application it hosts.

References:
ARS: SI-7.0
NIST 800-53: SI-7
PISP: 4.2.6.7

Related CSRs: 1.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Programmed integrity verification routines or checks are, for the most part, the most critical and comprehensive way to ensure the integrity of Medicare data.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs integrity verification software on the information system to look for evidence of information tampering, errors, and omissions.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes).
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs tools to automatically monitor the integrity of the information system and the applications the system hosts.
4. Examine information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system detects and protects against unauthorized changes to software and information on an ongoing basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software and information integrity control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Application System Accuracy Controls***

General Requirement

Control Technique

9.8 Programmed validation and edit checks shall identify erroneous data.

9.8.5 Data integrity and validation controls are used to provide assurance that Medicare information has not been altered and the system functions as intended.

References:
ARS: SI-7.CMS-1
ARS: SI-7.CMS-2
NIST 800-53: SI-7
PISP: 4.2.6.7

Related CSRs: 1.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Data integrity and validation controls are, for the most part, the most critical and comprehensive way to ensure the integrity of Medicare data, and ensure the system functions as intended.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs integrity verification software on the information system to look for evidence of information tampering, errors, and omissions.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes).
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs tools to automatically monitor the integrity of the information system and the applications the system hosts.
4. Examine information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system detects and protects against unauthorized changes to software and information on an ongoing basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software and information integrity control are documented and the resulting information used to actively improve the control on a continuous basis.

9.8.6 The integrity of software and information is reassessed by performing quarterly integrity scans of the system. Automated tools are employed that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.

References:
NIST 800-53: SI-7

Related CSRs: 2.1.1, 10.2.4, 10.2.5, 10.2.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs integrity verification software on the information system to look for evidence of information tampering, errors, and omissions.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes).
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs tools to automatically monitor the integrity of the information system and the applications the system hosts.
4. Examine information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system detects and protects against unauthorized changes to software and information on an ongoing basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software and information integrity control are documented and the resulting information used to actively improve the control on a continuous basis.

9.9 When appropriate, preformatted computer workstation screens shall be used for data entry.

9.9.1 Preformatted computer workstations screens are utilized and allow prompting for data to be entered and editing of data as it is entered.

References:
FISCAM: TAY-1.2

Related CSRs: 9.4.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach is to have needed data entry information and workstation screens succinctly formatted to facilitate ease of data entry. Standards do promote efficiency and accuracy.

Protocols: 1. Interview the system administrator to confirm that the required feature is universally available..
2. Observe a sample of workstation screens as personnel are processing data.
3. Review documented procedure specifying preformatted workstation screens, and describing screen prompts.

10. Network

10.1 LAN/Computer Room Access Controls shall be in place.

10.1.1 Controls are established to protect access authorization lists to secure areas such as data centers.

References:
CMS: Directed

Related CSRs: 2.2.17

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that only personnel with a need-to-know have access to the list.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming control of access lists in accordance with documented procedures.
3. By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center.

10.1.2 Physical access to enclosures housing network equipment is restricted. Access to telephone closets and information system distribution and transmission lines within organizational facilities is restricted to prevent eavesdropping, in-transit modification, disruption, or physical tampering. Access is granted to authorized personnel only, and access is monitored and recorded.

References:
ARS: PE-3.CMS-3
ARS: PE-4.CMS-1
CMS: Directed
NIST 800-53: PE-3
NIST 800-53: PE-4
PISP: 4.2.2.3
PISP: 4.2.2.4

Related CSRs: 2.2.1, 5.1.4, 5.9.14

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that access to the area where the network equipment is located is controlled.

Protocols: 1. Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
2. Examine organizational records or documents and the facility where the information system resides to determine if the organization controls physical access to information system distribution and transmission lines to prevent accidental damage, eavesdropping, in-transit modification, disruption, or physical tampering.
3. Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
4. Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST SP 800-76 (where the token-based access control function employs biometric verification).
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access and transmission medium controls are implemented.
6. Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently controls physical access to the facility, and to system distribution and transmission lines on an ongoing basis.
7. Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the facility access controls and the transmission medium controls are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Network***

General Requirement

Control Technique

10.2 Network system security shall be monitored for deficiencies.

10.2.1 The information system is configured to automatically verify the correct operation of system security functions upon system startup and restart, upon command by users with appropriate access, and at least on a monthly routine basis; and to notify system administration upon detection of security anomalies. Automated mechanisms are employed to support centralized management of distributed security testing and to provide centralized notification of failed automated security tests.

References:

ARS: SI-6.0
ARS: SI-6.1
ARS: SI-6.2
NIST 800-53: SI-6
PISP: 4.2.6.6

Related CSRs: 4.2.3, 10.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Automated mechanisms should be used to verify security functions.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system verifies the correct operation of security functions upon system startup and restart, and/or upon command by users with appropriate privileges.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system notifies the system administrator, shuts the system down, or restarts the system when anomalies are discovered.
3. Examine the system configuration to determine if it verifies the correct operations of security functions upon system startup and restart, upon command by user with appropriate privilege, periodically and notifies system administrator, shuts the system down, restarts the system when anomalies are discovered.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security functionality verification control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently verifies the security functionality within the system on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to provide notification of failed security tests to appropriate personnel.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms to support management of distributed security testing.

Category: ***Network***

General Requirement

Control Technique

10.2 Network system security shall be monitored for deficiencies.

10.2.2 Real-time file scanning is enabled. Desktop malicious code scanning software is installed, real-time protection and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every 12 hours. Malicious code scanning software is provided at critical entry points, such as remote-access servers.

References:

ARS: SI-3.CMS-1
CMS: Directed
NIST 800-53: SI-3
PISP: 4.2.6.3

Related CSRs: 1.13.8, 1.13.9, 5.12.1, 10.8.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A formal virus protection program should be established at the Network level.

Protocols: 1. Examine organizational records or documents to determine if the organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).
2. Interview selected organizational personnel with system and information integrity responsibilities and examine malicious code protection mechanisms to determine if the mechanisms detect and eradicate malicious code transported: (i) by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes, or compact discs), or other common means; or (ii) by exploiting information system vulnerabilities.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software).
4. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the malicious code protection control is implemented.
6. Examine malicious code protection mechanisms to determine if the mechanisms are: (i) appropriately updated to include the latest malicious code definitions; (ii) configured to perform periodic scans of the information system as well as real-time scans of each file as it is downloaded, opened, or executed; and (iii) configured to disinfect and quarantine infected files.
7. Examine electronic mail clients and servers to determine if the clients and servers are configured to block attachments with file extensions associated with malicious code (e.g., .pifi .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe).
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently applies malicious code protection measures within the information system on an ongoing basis.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the malicious code protection control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization centrally manages malicious code protection mechanisms employed in organizational information systems.
11. Examine the information system configuration to determine if the malicious code protection mechanisms are configured to download and install updates automatically directly from the vendor or some other trusted source.

Category: ***Network***

General Requirement

Control Technique

10.2 Network system security shall be monitored for deficiencies.

10.2.3 Network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed on demand, and at least once every 24 hours, to identify anomalies. Alerts are generated for review and assessment by technical staff.

Related CSRs: 5.12.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AU-6.CMS-2
ARS: SI-4.CMS-2
NIST 800-53: AU-6
NIST 800-53: SI-4
PISP: 4.2.6.4
PISP: 4.3.3.6

Guidance: Anomalies should be carefully analyzed to determine if unauthorized activity is occurring. Timely alerts are needed to initiate appropriate activities.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools.
2. Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
3. Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.
4. Examine intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies.
5. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.
7. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis.
9. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system monitoring tools and techniques control are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization provides the capability through the employment of automated tools, to immediately investigate, report, and respond to suspicious activity in real-time.
12. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms.
13. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.
14. Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.
15. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.

10.2 Network system security shall be monitored for deficiencies.

10.2.4 Intrusion detection software is implemented providing real-time identification of unauthorized use, misuse, and abuse of computer assets by internal network users and external hackers. IDS devices are installed at network perimeter points and host-based IDS sensors on critical servers.

References:
ARS: SI-4.2
ARS: SI-4.CMS-1
CMS: Directed
NIST 800-53: SI-4
PISP: 4.2.6.4

Related CSRs: 2.6.1, 9.8.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Intrusion-detection mechanisms should be monitoring the system constantly. Failsafes and processes to minimize the failure of the primary security measures should be in place at all times.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools.
2. Examine intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system monitoring tools and techniques control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs a centrally managed, systemwide intrusion detection capability.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization provides the capability through the employment of automated tools, to immediately investigate, report, and respond to suspicious activity in real-time.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms.
10. Examine organizational records or documents to determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware.
11. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.

10.2.5 The information system is protected against denial-of-service attacks as defined on the following sites or within the following documents: (1) SANS Organization (www.sans.org/dosstep); (2) SANS Organization's Roadmap to Defeating DDoS; and (3) NIST CVE List. Measures are in-place to limit the effects of information flooding types of denial-of-service attacks. The ability of users to launch denial-of-service attacks against other information systems or networks is also restricted.

References:
ARS: SC-5.0
ARS: SC-5.1
ARS: SC-5.2
NIST 800-53: SC-5
PISP: 4.3.4.5

Related CSRs: 9.8.6, 10.8.8

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A process should be established to check these sites on a regular basis.

Protocols: 1. Examine organizational records or documents (including developer design documentation) to determine if the information system protects against or limits the effects of the organization-defined types of denial of service attacks.
2. Examine organizational records or documents to determine if the organization uses automated tools to protect against or limit the effects of organization-defined types of denial of service attacks.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the denial of service protection control is implemented.
4. Test the denial of service protection by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo).
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization consistently implements denial of service protection for the information system on an ongoing basis.
6. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the denial of service protection control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.
8. Test the denial of service protection for the information system by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo).

10.2 Network system security shall be monitored for deficiencies.

10.2.6 Individual IDS devices are connected to a common IDS management network using common protocols. Automated tools are employed to integrate intrusion detection tools into access control mechanisms to enable rapid response to attacks through the re-configuration of IDS settings to support attack isolation and elimination.

References:
ARS: SI-4.1
ARS: SI-4.3
NIST 800-53: SI-4
PISP: 4.2.6.4

Related CSRs: 2.6.1, 9.8.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Automated tools should be employed to integrate intrusion detection tools that allow for rapid response to attacks.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools.
2. Examine intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system monitoring tools and techniques control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs a centrally managed, systemwide intrusion detection capability.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization provides the capability through the employment of automated tools, to immediately investigate, report, and respond to suspicious activity in real-time.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms.
10. Examine organizational records or documents to determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware.
11. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.

10.2.7 Stateful inspection and application firewall hardware and software are used. Firewalls from at least two (2) different vendors are used at various levels within the network. The operational failure of boundary protection mechanisms does not allow the unauthorized release of information outside of the information system boundary.

References:
ARS: SC-7.CMS-3
ARS: SC-7.CMS-4
NIST 800-53: SC-7
PISP: 4.3.4.7

Related CSRs: 10.8.1, 10.8.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that the stateful inspection capability is being properly utilized. Stateful inspection firewalls are third-generation firewalls that analyze packets at all OSI layers. Can be used to track connectionless protocols like UDP.

Protocols: 1. Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary protection control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the boundary protection control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Category: ***Network***

General Requirement

Control Technique

10.2 Network system security shall be monitored for deficiencies.

10.2.8 Logging on perimeter devices, including firewalls and routers, is enabled. Packet screening denials originating from untrusted networks, packet screening denials originating from trusted networks, proxy use denials, user account management, modification of packet filters, modification of proxy services, application errors, system shutdown and reboot, and system errors are recorded.

Related CSRs: 2.3.2, 10.8.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AU-2.CMS-1
ARS: SI-11.0
ARS: SI-12.1
NIST 800-53: AU-2
NIST 800-53: SI-11
NIST 800-53: SI-12
PISP: 4.2.6.11
PISP: 4.2.6.12
PISP: 4.3.3.2

Guidance: Ensure that records from perimeter devices contain the required information, and that they are carefully reviewed on a frequent basis.

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.
2. Test the information system by attempting to perform actions that are configured to generate an audit record.
3. Examine the information system to determine if the system identifies and handles error conditions in an expeditious manner.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events and error handling controls are implemented.
5. Examine the information system to determine if the system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries.
6. Examine the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel).
7. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures.
8. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis.
9. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently handles error conditions on an ongoing basis.
10. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events and error handling controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.
12. Examine the information system audit trail to determine if the system accurately compiles audit records from multiple components.
13. Test the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.
14. Examine organizational records or documents to determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.
15. Test the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.

Category: *Network*

General Requirement

Control Technique

10.2 Network system security shall be monitored for deficiencies.

10.2.9 Selected information system elements at critical control points (e.g., servers) provide records of user network and system activity. System audit records are reviewed on demand, and at least once every 24 hours, for: (1) initialization sequences, (2) logons and errors, (3) system processes and performance, and (4) system resources utilization to determine anomalies. Alert notifications are generated for technical staff review and assessment. Automated mechanisms are employed to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Related CSRs: 1.9.7, 2.1.8, 2.1.12, 2.1.14, 2.6.1, 5.9.1, 5.9.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AU-6.1
ARS: AU-6.CMS-1
ARS: CA-7.CMS-1
ARS: SI-4.2
CMS: Directed
NIST 800-53: AU-6
NIST 800-53: CA-7
NIST 800-53: SI-4
PISP: 4.1.4.7
PISP: 4.2.6.4
PISP: 4.3.3.6

Guidance: Ensure that records are kept of network activity. Establish a policy to review network infrastructure (i.e., routers, servers, etc.) system audit records for the required events.

Protocols: 1. Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
2. Examine organizational records or documents to determine if the organization monitors the security controls in the information system on an ongoing basis.
3. Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the continuous monitoring control is implemented.
6. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.
7. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis.
8. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
10. Test the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities by artificially generating auditable events and monitoring the results.
11. Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.
12. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization provides the capability through the employment of automated tools, to immediately investigate, report, and respond to suspicious activity in real-time.
13. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms.
14. Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.
15. Examine organizational records or documents to determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware.
16. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.

10.2 Network system security shall be monitored for deficiencies.

10.2.10 System error messages are revealed only to authorized users (e.g., system administrators, maintenance personnel). Confidential information (e.g., account numbers, UserIDs, social security numbers, etc.) are not listed in error records or associated administrative messages.

References:
ARS: SI-11.0
NIST 800-53: SI-11
PISP: 4.2.6.11

Related CSRs: 2.9.14

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that only authorized personnel with a need-to-know have access to system error messages and records.

Protocols: 1. Examine the information system to determine if the system identifies and handles error conditions in an expeditious manner.
2. Examine the information system to determine if the system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries.
3. Examine the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel).
4. Examine the information system to determine if the system lists sensitive information (e.g., account numbers, social security numbers, and Personally Identifiable Information [PII]) in error logs or associated administrative messages.
5. Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the error handling control is implemented.
7. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system consistently handles error conditions on an ongoing basis.
8. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the error handling control are documented and the resulting information used to actively improve the control on a continuous basis.

10.2.11 The use of resources is limited by priority to ensure that lower-priority processes do not interfere with the performance and/or completion of higher-priority processes running on the information system.

References:
ARS: SC-6
NIST 800-53: SC-6
PISP: 4.3.4.6

Related CSRs: 5.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The system should be configured to automatically limit the use of system resources by established priorities.

Protocols: 1. Examine organizational records or documents (including developer design documentation) to determine if information system resources have been prioritized and how the system limits the use of resources by priority.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that resource priority control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently limits the use of resources by priority on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the resource priority control are documented and the resulting information used to actively improve the control on a continuous basis.

10.3 Facsimile and e-mail shall be controlled.

10.3.1 Telephone numbers of the facsimile machines receiving sensitive information are verified before transmitting data.

References:
CMS: Directed
IRS 1075: 5.8@9.2.b

Related CSRs: 2.12.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A good approach might be a policy that requires verification of the receiving facsimile machine's telephone number.

Protocols: 1. Inspect records confirming conduct of the required verification.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

10.3.2 When sending or receiving sensitive fax information, a trusted staff member attends both the sending and receiving fax machines, or the fax machine is located in a locked room with custodial coverage over outgoing and incoming transmissions.

References:
CMS: Directed
IRS 1075: 5.8@9.2.a

Related CSRs: 2.12.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: a good approach might be a policy that states "If a locked room with custodial coverage is unavailable, trusted staff members are required to be at both the transmitting and receiving machines prior to transmittal."

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.

Category: ***Network***

General Requirement

Control Technique

10.3 Facsimile and e-mail shall be controlled.

10.3.3 Fax procedures are implemented for sensitive information require a cover sheet that explicitly provides guidance to the recipient, which includes: (1) notification of sensitive data and need for protection, and (2) notice to unintended recipients to telephone the sender, collect if necessary, to report the disclosure and confirm destruction of the information.

References:
CMS: Directed
IRS 1075: 5.8@9.2.c
IRS 1075: 5.8@9.2.c.1
IRS 1075: 5.8@9.2.c.2

Related CSRs: 1.4.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a formal procedure generating and attaching the required fax cover sheet.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.

10.3.4 Controls exist to identify and monitor appropriate use of the e-mail system by employees (including malware detection), and to enforce e-mail authentication, security, privacy, and message integrity. Outgoing e-mail messages and attachments are encrypted.

References:
ARS: SC-CMS-4.CMS-1
ARS: SI-4.4
CMS: Directed
NIST 800-53: SI-4
PISP: 4.2.6.4
PISP: 4.3.4.1

Related CSRs: 1.4.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.

Protocols: 1. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools.
2. Examine intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies.
3. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis.

10.3.5 Technical security measures are implemented for e-mail to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications network. If digital signatures are implemented, all outgoing e-mail messages are digitally signed and the digital signatures for received messages are verified.

References:
ARS: AU-10
ARS: SC-CMS-4.CMS-2
NIST 800-53: AU-10
PISP: 4.3.3.10
PISP: 4.3.4.1

Related CSRs: 2.2.24

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.

Protocols: 1. Examine the information system configuration to determine if the system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).
2. Test the information system's non-repudiation capability by: (i) demonstrating that when the non-repudiation capability is applied to a "test" action (e.g., create information, send a message, approve information (e.g., to indicate concurrence or sign a contract]), the organization can determine whether a given individual took the particular action and, when applicable, whether a given individual received something as a result of the action (e.g., received a message as a result of the action); and (ii) by demonstrating that it is not possible to alter or spoof the responsible individual's identity for a given action.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the non-repudiation control is implemented.
4. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently provides a non-repudiation capability on an ongoing basis.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the non-repudiation control are documented and the resulting information used to actively improve the control on a continuous basis.

10.3 Facsimile and e-mail shall be controlled.

10.3.6 Audit reviews include checks, to assure that system administrators and others with special system-level access privileges are prohibited from reading the e-mail messages of others unless authorized on a case-by-case basis by appropriate management officials.

References:
ARS: AU-2.0
CMS: Directed
NIST 800-53: AU-2
PISP: 4.3.3.2

Related CSRs: 2.1.11, 2.1.12

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Ensure that policy exists and it contains the necessary checks with regards to audit reviews.

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.
2. Test the information system by attempting to perform actions that are configured to generate an audit record.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented.
4. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis.
5. Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.
7. Examine the information system audit trail to determine if the system accurately compiles audit records from multiple components.
8. Test the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.
9. Examine organizational records or documents to determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.
10. Test the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.

10.4 Cryptographic tools shall be controlled.

10.4.1 Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs when no other means of protection exists.

References:
FISCAM: TAC-3.3
HIPAA: 164.312(a)(2)(iv)
HIPAA: 164.312(e)(2)(ii)

Related CSRs: 1.9.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: In some cases—especially those involving telecommunications—it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs, both while these data and programs are “in” the computer system and while they are being transmitted to another computer system or stored on removable media, such as floppy disks, which may be held in a remote location.

Protocols: 1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation establishing that the required protection has been implemented.

10.4.2 The use of application security mechanisms, such as SSL and SSH, is both enabled and forced. CMS-approved encryption and password authentication methods are used in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).

References:
ARS: SC-CMS-3.CMS-1
ARS: SC-CMS-3.CMS-2
PISP: 4.3.4.1

Related CSRs: 10.5.1, 10.6.1, 10.8.2, 10.8.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Protocols: 1. Review existing policies and procedures to ensure requirements of CSR specified.
2. Test security mechanisms on a periodic basis for proper operation.
3. Review mechanisms against risk assessment to identify changes required to existing mechanisms.

Category: ***Network***

General Requirement

Control Technique

10.4 Cryptographic tools shall be controlled.

10.4.3 If encryption is used as an access control mechanism or as authentication to a cryptographic module, it must meet FIPS-validated encryption module (i.e., a minimum of Triple Data Encryption Algorithm (TDEA) encryption with a 128-bit key).

References:

ARS: AC-3.CMS-1
ARS: AC-3.CMS-2
ARS: IA-7.0
NIST 800-53: AC-3
NIST 800-53: IA-7
PISP: 4.3.1.7
PISP: 4.3.2.3

Related CSRs: 10.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management. Only a FIPS-validated encryption module at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key shall be used. An updated list of FIPS-approved modules is available on the NIST web site for each approved encryption algorithm.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the system employs authentication methods for authentication to a cryptographic module that meet the requirements of FIPS 140-2.
2. Examine organizational records or documents and information system configuration settings to determine if the information system employs authentication methods in accordance with FIPS 201 and NIST SP 800-73 and 800-78 when the cryptographic module is a personal identity verification (PIV) card token.
3. Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented.
5. Examine organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic module authentication control is implemented.
7. Examine organizational records or documents to determine if the organization clearly documents authentication methods to a cryptographic module for the information system.
8. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently meets the requirements of FIPS 140-2 for cryptographic module authentication on an ongoing basis.
9. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic module authentication control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Network***

General Requirement

Control Technique

10.4 Cryptographic tools shall be controlled.

10.4.4 Sensitive data being electronically transmitted outside of a secured network must be protected from source to destination using a FIPS-approved encryption standard, and data must be transmitted via secured communications. Cryptographic mechanisms are employed to ensure recognition of changes and to prevent unauthorized disclosure of information during transmission.

Related CSRs: 10.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AC-4.CMS-2
ARS: SC-8.1
ARS: SC-8.CMS-1
ARS: SC-9.1
ARS: SC-9.CMS-1
FISCAM: TAC-3.2.E.1
HIPAA: 164.312(a)(2)(iv)
HIPAA: 164.312(e)(2)(ii)
IRS 1075: 5.8@1.1
IRS 1075: 5.8@1.2
IRS 1075: 5.8@1.3
NIST 800-53: AC-4
NIST 800-53: SC-8
NIST 800-53: SC-9
PISP: 4.3.2.4
PISP: 4.3.4.8
PISP: 4.3.4.9

Guidance: Ensure that a means of protecting sensitive information during transmittal has been implemented. Guided media is generally acceptable for internal transmissions within protected facilities. Encryption is typically required for transmission outside of protected facilities or through uncontrolled or public facilities or systems.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system protects the confidentiality of transmitted information and how the confidentiality protections are implemented (i.e., mechanisms, tools, techniques, and technologies).
2. Examine information system interconnection agreements to determine if the agreements address: (i) the types of permissible and impermissible flow of information between systems; and (ii) the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.
3. Examine information system configuration settings to determine if controls are in place to restrict the flow of information within the system and between interconnected systems in accordance with the applicable policy, procedures, and assigned authorizations.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the transmission confidentiality and integrity controls are implemented.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently protects the confidentiality and integrity of transmitted information on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems on an ongoing basis.
7. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission confidentiality and integrity controls are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information flow enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.
9. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).
10. Examine organizational records or documents (including developer design documentation) to determine how the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).
11. Test the cryptographic mechanisms employed in the information system used to achieve transmission confidentiality and integrity by attempting to exploit any known vulnerabilities.

Category: ***Network***

General Requirement

Control Technique

10.4 Cryptographic tools shall be controlled.

10.4.5 When cryptography is required and employed, automated mechanisms with supporting procedures, or manual procedures for cryptographic key establishment and key management are employed. The mechanisms and procedures comply with CMS-approved cryptography standards.

References:
ARS: SC-12.CMS-1
NIST 800-53: SC-12
PISP: 4.3.4.12

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and management and how the mechanisms and procedures are implemented.
2. Test the information system cryptographic key establishment and management by using the automated mechanisms to walk a test key through all the phases of its lifecycle from generation to revocation.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic key establishment and management control is implemented.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently employs automated mechanisms with supporting procedures or the organization employs manual procedures for cryptographic key establishment and management on an ongoing basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic key establishment and management control are documented and the resulting information used to actively improve the control on a continuous basis.

10.4.6 When cryptography is required and employed, the organization complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 which requires the information system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

References:
ARS: SC-13
NIST 800-53: SC-13
PISP: 4.3.4.13

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management. Only a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key shall be used.

Protocols: 1. Examine organizational records or documents (including developer design documentation) to determine if the employed cryptography complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the use of validated cryptography control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization consistently uses validated cryptography within the information system on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the use of validated cryptography control are documented and the resulting information used to actively improve the control on a continuous basis.

10.4 Cryptographic tools shall be controlled.

10.4.7 If public key certificates are used: (1) a certificate policy and certification practice statement is developed and implemented for the issuance of public key certificates; (2) the issuance of public key certificates to individuals is authorized by a supervisor or other appropriate Business Partner official; and (3) the issuance of public key certificates to individuals is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

References:
ARS: SC-16
ARS: SC-17
NIST 800-53: SC-16
NIST 800-53: SC-17
PISP: 4.3.4.16
PISP: 4.3.4.17

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system and how the policy is implemented in the information system.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the public key infrastructure certificates control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization consistently develops and implements a certificate policy and certification practice statement for use in issuing public key certificates on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the public key infrastructure certificates control are documented and the resulting information used to actively improve the control on a continuous basis.

10.5 Adequate Network password policies shall be implemented.

10.5.1 For password-based authentication, passwords are protected from disclosure and modification, and encrypted when stored and when transmitted outside the LAN/WAN.

References:
ARS: IA-5.0
FISCAM: TAC-3.2.A.7
FISCAM: TAC-3.2.E.1
NIST 800-53: IA-5
PISP: 4.3.1.5

Related CSRs: 10.4.2, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that passwords are not transmitted as plain-text.

Protocols: 1. Examine organizational records or documents and the information system configuration settings to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.
2. Examine organizational records or documents to determine if the organization establishes administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Examine organizational records or documents to determine if the organization changes default authenticators upon information system installation.
4. Interview selected organizational personnel with identification and authentication responsibilities to determine if users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.
5. Examine organizational records or documents to determine if the information system establishes user control of the corresponding private key and maps the authenticated identity to the user account (for PKI-based authentication).
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator management control is implemented.
7. Test the information system to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.
8. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently manages authenticators for the information system on an ongoing basis.
9. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator management control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Network***

General Requirement

Control Technique

10.6 Internet Security Policies shall be made available.

10.6.1 CMS Business Partner's Internet connections must be in accordance with Section 5 in the CMS Business Partners Systems Security Manual. When a determination for Internet use has been made, it shall include a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key.

References:
ARS: IA-7.0
CMS: Directed
PISP: 4.3.1.7

Related CSRs: 10.4.2, 10.4.3, 10.4.4, 10.8.1, 10.8.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: At present, the internet may not be used for CMS sensitive data.

Protocols: 1. Review documentation describing the approved authentication process used to allow establishment of the virtual private network connection to a local network or other system carrying sensitive information.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation describing protections to assure that the only interconnections allowed between the Internet and networks carrying sensitive information are the specified virtual private network connections.
4. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement.

10.6.2 Clear privacy policies are posted on web sites, at major entry points to a web site, and on any web page where substantial personal information from the public is collected.

References:
ARS: AC-8.CMS-4
CMS: Directed
NIST 800-53: AC-8
PISP: 4.3.2.8

Related CSRs: 1.4.6, 1.7.1, 2.1.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Privacy policy banners should be displayed on web pages where personal information is collected. The eGov Act of 2002 and OMB M03-22 guidance requires that agencies post privacy policies on public websites.

Protocols: 1. Examine the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries).
2. Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.
4. Test the system use notification message by accessing the login screen for the information system to determine if it remains on the screen until the user takes explicit actions to log on to the information system.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.

10.6.3 Unless prior approval by CMS is obtained in writing, persistent cookies are prohibited.

References:
ARS: SC-CMS-5.CMS-1
PISP: 4.3.4.1

Related CSRs: 1.13.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The absence of persistent cookies should be verifiable. A persistent cookie has an expiration date and is stored on your disk until that date. A persistent cookie can be used to track a user's browsing habits by identifying him whenever he returns to a site. Information about where you come from and what web pages you visit already exists in a web server's record files and could also be used to track users browsing habits, cookies just make it easier.

Protocols: 1. Review software configuration records/procedures.
2. If not currently in place, procedures to delete cookies should be developed and personnel trained on procedures.

10.6 Internet Security Policies shall be made available.

10.6.4 User responsibilities and expectations for Internet use are defined; and organizational sanctions for violations are developed, implemented, and enforced. Technical security controls are implemented to prevent users from accessing inappropriate Internet content.

References:
ARS: PS-8
NIST 800-53: PS-8
PISP: 4.2.1.8

Related CSRs: 10.8.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: At present, the internet may not be used for CMS sensitive data.

Protocols: 1. Examine organizational records or documents to determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
2. Examine organizational records or documents including signed rules of behavior to determine if the organization defines and conveys the formal sanctions process to organizational personnel.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel sanctions control is implemented.
4. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently employs and monitors personnel sanctions on an ongoing basis.
5. Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel sanctions control are documented and the resulting information used to actively improve the control on a continuous basis.

10.7 Configuration Control Policy shall be documented and available.

10.7.1 Purchased software is used in accordance with contract agreements and copyright laws. Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software.

References:
ARS: SA-6
CMS: Directed
NIST 800-53: SA-6
PISP: 4.1.3.6

Related CSRs: 1.1.5, 1.13.3, 6.5.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A formal program should be established regarding the use of purchased software.

Protocols: 1. Examine organizational records or documents to determine if the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software usage restrictions control is implemented.
3. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently enforces software usage restrictions on an ongoing basis.
4. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software usage restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Network***

General Requirement

Control Technique

10.7 Configuration Control Policy shall be documented and available.

10.7.2 Change control is implemented to authorize, enforce, and maintain control of changes to hardware, software, and security mechanisms. The change control mechanism documents system changes, enforces individual accountability, and provides sufficient detail to reverse or undo changes.

Related CSRs: 1.9.3, 3.4.1, 5.9.4, 6.3.1, 6.3.5, 6.3.13, 6.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: CM-5.1
CMS: Directed
NIST 800-53: CM-3
NIST 800-53: CM-5
NIST 800-53: CM-6
PISP: 4.2.4.3
PISP: 4.2.4.5

Guidance: A good approach might be to establish change control policies and procedures for all hardware, software, and security products.

Protocols: 1. Examine organizational records or documents to determine if the organization documents and controls changes to the information system.
2. Examine organizational records or documents to determine if appropriate organizational officials approve information system changes in accordance with organizational policy and procedures.
3. Examine organizational records or documents to determine if the organization maintains a list of personnel authorized to access the information system for purposes of initiating changes, upgrades, and/or modifications to the system.
4. Examine organizational records or documents to determine if the organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.
5. Examine organizational records or documents to determine if the organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.
6. Examine organizational records or documents identifying changes made to the information system to determine if only authorized personnel initiated, tested, approved, and implemented changes to the system.
7. Examine selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings.
8. Examine organization documentation or records to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration settings control is implemented.
9. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies, documents, and controls information system configuration changes on an ongoing basis.
10. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration change and setting controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently enforces physical and logical access to the information system for purposes of change control on an ongoing basis.
12. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access restrictions for change control are documented and the resulting information used to actively improve the control on a continuous basis.
13. Examine organizational records or documents to determine if the organization employs automated mechanisms to manage configuration changes to the information system
14. Examine organizational records or documents to determine if the organization employs automated mechanisms to enforce access restrictions and to support auditing of the enforcement of actions.
15. Examine output generated by the information system to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
16. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.
17. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to enforce access restrictions and to support auditing of the enforcement of actions.
18. Examine organizational records or documents to determine if the organization: (i) restricts access to automated mechanism(s) to authorized employees only; and (ii) tracks all activities performed by employees using the automated mechanism(s) to support auditing of the enforcement actions.
19. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to centrally manage, apply, and verify configuration settings.

Category: ***Network***

General Requirement

Control Technique

10.7 Configuration Control Policy shall be documented and available.

10.7.3 A current baseline configuration of the information system is developed, documented, and maintained. The baseline configuration documents the system's: (1) purpose; (2) description; (3) technical operations; (4) technical access; (5) maintenance; and (6) personnel training requirements (including administrators and users).

References:

ARS: CM-2.1
ARS: CM-2.CMS-1
ARS: SA-5.CMS-1
NIST 800-53: CM-2
NIST 800-53: SA-5
PISP: 4.1.3.5
PISP: 4.2.4.2

Related CSRs: 1.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The configuration of the information system is consistent with the Federal Enterprise Architecture and the CMS Target Architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).

Protocols: 1. Examine organizational records or documents to determine if the organization develops, documents, and maintains a baseline configuration of the information system which includes key architectural components and the relationship among those components.
2. Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
3. Examine organizational records or documents to determine if the organization develops, documents, and maintains an inventory of the hardware, software, and firmware components that compose the information system and ownership information by component.
4. Examine organizational records or documents to determine if the inventory of information system components designates those components required to implement and/or conduct contingency operations.
5. Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the baseline configuration and information system documentation controls are implemented.
7. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently manages the baseline configuration of the information system on an ongoing basis.
8. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.
9. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the baseline configuration control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.
11. Examine organizational records or documents to determine if the organization identifies: (i) instances that trigger baseline configuration and component inventory updates; (ii) the frequency of updates to the baseline configuration and component inventory; (iii) the dates of baseline configuration and inventory updates, a summary of the updates, and the name of the individuals performing the updates.
12. Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.
13. Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Category: ***Network***

General Requirement

Control Technique

10.7 Configuration Control Policy shall be documented and available.

10.7.4 The baseline configuration, system component inventory, and any other information system-related operations or security documentation is reviewed and, if necessary, updated at least once per year, and while planning major system changes/upgrades. Automated mechanisms are employed to maintain an up-to-date, complete, accurate, and readily available baseline configuration. The baseline configuration and component inventory is updated as an integral part of information system component installations.

References:

ARS: CM-2.1
ARS: CM-2.2
ARS: CM-2.CMS-1
NIST 800-53: CM-2
NIST 800-53: CM-8
PISP: 4.2.4.2

Related CSRs: 1.9.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The configuration of the information system is consistent with the CMS Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).

Protocols: 1. Examine organizational records or documents to determine if the organization develops, documents, and maintains a baseline configuration of the information system which includes key architectural components and the relationship among those components.
2. Examine organizational records or documents to determine if the organization develops, documents, and maintains an inventory of the hardware, software, and firmware components that compose the information system and ownership information by component.
3. Examine organizational records or documents to determine if the inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).
4. Examine organizational records or documents to determine if the inventory of information system components designates those components required to implement and/or conduct contingency operations.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the baseline configuration and system component inventory control is implemented.
6. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently manages the baseline configuration and component inventory of the information system on an ongoing basis.
7. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the baseline configuration and system component inventory control are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the organization identifies: (i) instances that trigger baseline configuration and component inventory updates; (ii) the frequency of updates to the baseline configuration and component inventory; (iii) the dates of baseline configuration and inventory updates, a summary of the updates, and the name of the individuals performing the updates.
9. Examine organizational records or documents to determine if the organization employs automated mechanisms to manage the information system baseline configuration and system component inventory functions.
10. Test the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that baseline configuration and system component inventory updates are scheduled and conducted as required.
11. Examine organizational records or documents to determine if the log of baseline configuration and system component inventory updates for the information system is up-to-date, accurate, complete, and available to appropriate organizational personnel.

Category: ***Network***

General Requirement

Control Technique

10.7 Configuration Control Policy shall be documented and available.

10.7.5 Automated mechanisms are employed to: (1) document proposed changes to the information system; (2) notify appropriate approval authorities; (3) identify approvals that have not been received in a timely manner; (4) inhibit change until necessary approvals are received; and (5) document completed changes to the information system.

References:
ARS: CM-3.1
NIST 800-53: CM-3
PISP: 4.2.4.3

Related CSRs: 3.5.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes.

Protocols: 1. Examine organizational records or documents to determine if the organization documents and controls changes to the information system.
2. Examine organizational records or documents to determine if appropriate organizational officials approve information system changes in accordance with organizational policy and procedures.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration change control is implemented.
4. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently documents and controls information system configuration changes on an ongoing basis.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration change control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents to determine if the organization employs automated mechanisms to manage configuration changes to the information system
7. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

10.7.6 When changes to the system occur, the installation of information system components is recorded in the appropriate system documentation resource(s). Security impact analyses are conducted to determine the effects of system changes. As part of the security impact analyses, the system security features and audit activities associated with configuration changes to the information system are validated to ensure they still function properly.

References:
ARS: CM-4.CMS-1
NIST 800-53: CM-4
NIST 800-53: CM-5
PISP: 4.2.4.4

Related CSRs: 1.9.7, 1.12.5, 4.1.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The organization documents the installation of information system components. After the information system is changed, the organizations checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.

Protocols: 1. Examine organizational records or documents to determine if the organization monitors changes to the information system and identifies the types of changes monitored.
2. Examine organizational records or documents to determine if the organization performs security impact analyses to assess the effects of changes to the information system.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring configuration changes control is implemented.
4. Examine organizational records or documents to determine if the organization employs automated mechanisms to enforce access restrictions and to support auditing of the enforcement of actions.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently monitors configuration changes to the information system on an ongoing basis.
6. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to enforce access restrictions and to support auditing of the enforcement of actions.
7. Examine organizational records or documents to determine if the organization: (i) restricts access to automated mechanism(s) to authorized employees only; and (ii) tracks all activities performed by employees using the automated mechanism(s) to support auditing of the enforcement actions.
8. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring configuration changes control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Network***

General Requirement

Control Technique

10.7 Configuration Control Policy shall be documented and available.

10.7.7 The integrity of critical files and directories is reviewed for unexpected and unauthorized changes at least daily. The review of file creation, changes, and deletions is automated; permission changes are monitored. Alert notifications are generated for technical staff review and assessment.

References:
ARS: AC-13.CMS-1
NIST 800-53: AC-13
PISP: 4.3.2.13

Related CSRs: 3.6.1, 3.6.4, 3.6.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Procedures and/or an automated system for file integrity review and alert generation should be available and kept current. Files to be inspected include system code, application code, configuration and security related files.

Protocols: 1. Interview selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system.
2. Examine organizational records or documents to determine if unusual activity is investigated, reported to appropriate officials, and resolved.
3. Examine organizational records of supervisory notices or disciplinary actions to users to determine if the organization is supervising user activities regarding the use and application of information system access controls.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the supervision and review of access control is implemented.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently supervises and reviews user activities with respect to the enforcement and use of access controls for the information system on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the supervision and review of access control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities and how those mechanisms are implemented.
8. Examine the configuration of the automated mechanism(s) within the information system to determine if the mechanisms support the review of user activities.
9. Examine the output from the automated mechanism(s) within the information system to determine if each of the automated functions associated with the review of user activities produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.

10.7.8 Physical and logical access restrictions are enforced to limit changes to the information system. Controls are implemented and/or enabled to limit public and employee access to system-level software and administrator tools, scripts, and utilities. Automated mechanisms are employed to enforce access restrictions and to support auditing of the enforcement actions.

References:
ARS: CM-5.1
ARS: CM-5.CMS-1
NIST 800-53: CM-5
PISP: 4.2.4.5

Related CSRs: 2.1.4, 2.9.2, 3.1.3, 3.2.3

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The organization documents changes to information system components. The organization audits activities associated with configuration changes to the information system.

Protocols: 1. Examine organizational records or documents to determine if the organization maintains a list of personnel authorized to access the information system for purposes of initiating changes, upgrades, and/or modifications to the system.
2. Examine organizational records or documents to determine if the organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.
3. Examine organizational records or documents identifying changes made to the information system to determine if only authorized personnel initiated, tested, approved, and implemented changes to the system.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access restrictions for change control is implemented.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently enforces physical and logical access to the information system for purposes of change control on an ongoing basis.
6. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access restrictions for change control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Examine organizational records or documents to determine if the organization employs automated mechanisms to enforce access restrictions and to support auditing of the enforcement of actions.
8. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to enforce access restrictions and to support auditing of the enforcement of actions.
9. Examine organizational records or documents to determine if the organization: (i) restricts access to automated mechanism(s) to authorized employees only; and (ii) tracks all activities performed by employees using the automated mechanism(s) to support auditing of the enforcement actions.

10.7 Configuration Control Policy shall be documented and available.

10.7.9 The security settings of information technology products are configured to the most restrictive mode, based upon system operational requirements. The information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

References:
ARS: AC-6.CMS-5
ARS: CM-6.CMS-1
NIST 800-53: AC-6
NIST 800-53: CM-6
PISP: 4.2.4.6
PISP: 4.3.2.6

Related CSRs: 10.8.7, 10.8.8, 10.8.10

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: NIST SP 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.

Protocols: 1. Examine organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
2. Examine organizational records or documents to determine if the organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.
3. Examine organizational records or documents to determine what access rights/privileges the organization assigns to user tasks.
4. Examine selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings.
5. Examine selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks.
6. Examine organization documentation or records to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration settings control is implemented.
7. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces the most restrictive set of rights/privileges or accesses needed by users on an ongoing basis.
9. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies configuration settings to the information system on an ongoing basis.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least privilege and configuration settings controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Examine organizational records or documents to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
12. Examine output generated by the information system to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
13. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to centrally manage, apply, and verify configuration settings.

10.7.10 The use of mobile code on Medicare claims information systems or networks has been approved and the following controls are implemented: (1) usage restrictions and implementation guidance are established for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (2) the use of mobile code within the information system is authorized, monitored, and controlled.

References:
ARS: SC-18
NIST 800-53: SC-18
PISP: 4.3.4.17

Related CSRs:

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST SP 800-28 provides guidance on active content and mobile code.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; (ii) documents, monitors, and controls the use of mobile code within the information system; and (iii) requires organizational officials to approve the use of mobile code.
2. Test the information system by attempting to run mobile code in an application where it is specifically prohibited to determine if the organization implements mobile code usage restrictions.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the mobile code control is implemented.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if mobile code is consistently restricted on an ongoing basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the mobile code control are documented and the resulting information used to actively improve the control on a continuous basis.

Category: ***Network***

General Requirement

Control Technique

10.8 Logical Network Access Controls shall be in place.

10.8.1 Any connection to the Internet, or other external networks or systems, occurs through the use of appropriate control interfaces, including, but not limited to, firewalls, routers, gateways, proxies, and encrypted tunnels.

References:
CMS: Directed
FISCAM: TAC-3.2.E.1
IRS 1075: 5.8@6.1
IRS 1075: 5.8@6.2
IRS 1075: 5.8@6.3
NIST 800-53: SC-7
PISP: 4.3.4.7

Related CSRs: 1.13.6, 10.2.7, 10.6.1, 10.6.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A firewall must separate corporate computers and servers from the internet or other external networks or systems. Workstations and servers behind the corporate firewall must not have a modem connection. Modem connections will be handled via an authorized dial-in server.

Protocols: 1. Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary protection control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the boundary protection control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

10.8.2 Procedures for authentication are implemented to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; and (3) grant access to the functions of critical network devices.

References:
ARS: MA-4.0
CMS: Directed
HIPAA: 164.312(d)
NIST 800-53: MA-4
PISP: 4.2.5.4

Related CSRs: 2.9.8, 2.9.11, 5.9.13, 10.4.2, 10.10.2, 10.10.3, 10.10.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: A formal program should be established with a policy and procedure.

Protocols: 1. Examine organizational records or documents to determine if the organization approves, controls, and monitors remote access.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented.
3. Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently approves, monitors, and controls remote access on an ongoing basis.
4. Interview selected organizational personnel with remote access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Examine organizational records or documents to determine if: (i) the organization audits all remote access sessions and (ii) appropriate organizational personnel review the audit logs of the remote sessions.

Category: ***Network***

General Requirement

Control Technique

10.8 Logical Network Access Controls shall be in place.

10.8.3 The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored.

References:
ARS: AC-8.CMS-1
FISCAM: TAC-3.2.E.2.1
NIST 800-53: AC-8
PISP: 4.3.2.8

Related CSRs: 1.4.6, 1.4.7

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The choice of which screen warning banner to implement is up to the system owner and should be based on system-specific technology limitations, data sensitivity, or other unique system requirements.

Protocols: 1. Examine the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries).
2. Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.
4. Test the system use notification message by accessing the login screen for the information system to determine if it remains on the screen until the user takes explicit actions to log on to the information system.
5. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis.
6. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.

10.8.4 Workstations with dial-up access generate a unique identifier code before connection is completed.

References:
FISCAM: TAN-2.1.7

Related CSRs: 1.13.1, 7.4.1, 10.10.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: If workstations have dial-up access, ensure that a unique ID code is generated for each dial-up session.

Protocols: 1. Observe a sample of dial-up connections involving each type of access controller.
2. Review documented dial-up procedure to confirm inclusion of the required features.

10.8.5 All servers allowing public access (e.g. public web servers, public e-mail servers, public DNS servers) are placed within a DMZ, and direct access is not allowed to the internal network. In addition, the integrity and availability of publicly available information and applications on the servers is protected. DMZ servers cannot access the internal network. DMZ packet filtering and proxy rules are used to provide protection for servers.

References:
ARS: SC-14.CMS-2
ARS: SC-2.CMS-1
ARS: SC-7.1
NIST 800-53: SC-14
NIST 800-53: SC-2
NIST 800-53: SC-7
PISP: 4.3.4.14
PISP: 4.3.4.2
PISP: 4.3.4.7

Related CSRs: 2.3.2, 2.9.2, 10.2.8, 10.6.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The architecture and the use of rules should prohibit unauthorized access to all servers.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if, for publicly available information systems, the system protects the integrity of the information and applications and how the protections are implemented.
2. Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
3. Test the publicly available information system by attempting to alter protected information using a public account to determine if access is limited in order to preserve the integrity of the information and the applications.
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary and public access protection controls are implemented.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis.
6. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently protects the integrity of the information and applications on public access systems on an ongoing basis.
7. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the boundary and public access protection controls are documented and the resulting information used to actively improve the control on a continuous basis.
8. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Category: ***Network***

General Requirement

Control Technique

10.8 Logical Network Access Controls shall be in place.

10.8.6 All traffic for external communications is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required (i.e., deny all, permit by exception). The unauthorized release of information outside of the information system boundary or unauthorized communication through the information system boundary is prevented when there is an operational failure of the boundary protection mechanisms.

Related CSRs: 10.2.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

References:

ARS: AC-4.CMS-1
ARS: CM-7.1
ARS: SC-7.CMS-1
NIST 800-53: AC-4
NIST 800-53: CM-7
NIST 800-53: SC-7
PISP: 4.2.4.7
PISP: 4.3.2.4
PISP: 4.3.4.7

Guidance: The packet screening rules should apply only to specified firewalls and routers.

Protocols: 1. Examine organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.
2. Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
3. Examine information system interconnection agreements to determine if the agreements address: (i) the types of permissible and impermissible flow of information between systems; and (ii) the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.
4. Examine information system configuration settings to determine if controls are in place to restrict the flow of information within the system and between interconnected systems in accordance with the applicable policy, procedures, and assigned authorizations.
5. Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information flow enforcement, least functionality, and boundary protection controls are implemented.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems on an ongoing basis.
8. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies the concept of least functionality to the information system on an ongoing basis.
9. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis.
10. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information flow enforcement, least functionality, and boundary protection controls are documented and the resulting information used to actively improve the control on a continuous basis.
11. Examine organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.
12. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Category: ***Network***

General Requirement

Control Technique

10.8 Logical Network Access Controls shall be in place.

10.8.7 Automated mechanisms are employed centrally to apply and verify configuration settings. The information system is reviewed annually or on an incremental basis where all parts are addressed within a year, to identify and eliminate unnecessary functions, ports, protocols, and/or services.

References:
ARS: CM-6.1
ARS: CM-7.1
NIST 800-53: CM-6
NIST 800-53: CM-7
PISP: 4.2.4.6
PISP: 4.2.4.7

Related CSRs: 1.13.10, 10.7.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: NIST SP 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.
Information systems are capable of providing a wide variety of functions and services.
Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services provided by information systems should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Protocols: 1. Examine organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.
2. Examine organizational records or documents to determine if the organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.
3. Examine selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings.
4. Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.
5. Examine organization documentation or records to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration settings and least functionality controls are implemented.
6. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies configuration settings and the conept of least functionality to the information system on an ongoing basis.
7. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration settings and least functionality controls are documented and the resulting information used to actively improve the control on a continuous basis.
8. Examine organizational records or documents to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
9. Examine output generated by the information system to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
10. Examine organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.
11. Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to centrally manage, apply, and verify configuration settings.

10.8.8 The information system is specifically configured to prohibit and/or restrict the use of the functions, ports, protocols, and/or services as listed within the following documents/resource locations: (1) NIST Common Vulnerabilities and Exposures (www.cve.mitre.org/cve/); and (2) SANS List of Vulnerabilities (www.sans.org/top20/). All network protocols not explicitly required for system and application functionality are disabled.

References:
ARS: CM-7.0
ARS: CM-7.1
NIST 800-53: CM-7
PISP: 4.2.4.7

Related CSRs: 1.8.4, 2.3.1, 10.2.5, 10.7.9

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Develop and implement a way to verify that the protocols that are not required have been disabled.

Protocols: 1. Examine organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.
2. Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least functionality control is implemented.
4. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if the organization consistently applies the concept of least functionality to the information system on an ongoing basis.
5. Interview selected organizational personnel with configuration management responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least functionality control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Examine organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Category: ***Network***

General Requirement

Control Technique

10.8 Logical Network Access Controls shall be in place.

10.8.9 The information system uses either a shared secret (i.e., password) or digital certificate to identify and authenticate specific devices before establishing a connection.

References:
ARS: IA-3.0
NIST 800-53: IA-3
PISP: 4.3.1.3

Related CSRs: 10.4.2, 10.10.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.

Protocols: 1. Examine organizational records or documents and information system configuration settings to determine if the system uses either shared known information or an organizational authentication solution to identify and authenticate devices on local and/or wide area networks.
2. Examine organizational records or documents to determine if the strength of the device authentication mechanism is consistent with the FIPS 199 security categorization of the information system.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the device authentication and authentication control is implemented.
4. Test the information system to determine if the system identifies and authenticates specific devices before establishing connections to those devices.
5. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently identifies and authenticates devices prior to establishing connections on an ongoing basis.
6. Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the device identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.

10.8.10 The information system is configured to prohibit the remote activation of collaborative computing mechanisms (e.g., video and audio conferencing). The information system provides an explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone) which are authorized in writing by the CIO. Such authorized mechanisms are configured to provide a disconnection capability (either logically or physically) when not in use.

References:
ARS: SC-15.1
ARS: SC-15.CMS-1
NIST 800-53: SC-15
PISP: 4.3.4.15

Related CSRs: 10.7.9, 10.10.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Policies and procedures should exist that address these control objectives.

Protocols: 1. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone) and how remote activation of collaborative computing is prohibited.
2. Test the information system by attempting to remotely control video or audio capabilities to determine if remote activation of collaborative computing mechanisms is restricted.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the collaborative computing control is implemented.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information systems consistently implements restrictions on the use of collaborative computing on an ongoing basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the collaborative computing control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system provides physical disconnect of cameras and microphones in a manner that supports ease of use and how the information system provides physical disconnect of these components.

Category: ***Network***

General Requirement

Control Technique

10.8 Logical Network Access Controls shall be in place.

10.8.11 The number of access points to the information system is limited to allow for better monitoring of inbound and outbound network traffic. A managed interface (boundary protection devices in an effective security architecture) is implemented with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

References:
NIST 800-53: SC-7

Related CSRs: 1.11.4, 10.2.7, 10.10.2, 10.10.5

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks.

Protocols: 1. Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
2. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary protection control is implemented.
3. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis.
4. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the boundary protection control are documented and the resulting information used to actively improve the control on a continuous basis.
5. Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Category: ***Network***

General Requirement

Control Technique

10.9 Vulnerabilities to physical and cyber attacks shall be assessed.

10.9.1 Management-initiated penetration testing is performed as needed but at least annually, vulnerability scanning is performed at least quarterly, and an enterprise security posture review is conducted at least yearly. Findings and assessment results are documented and vulnerabilities are correlated to the Common Vulnerabilities and Exposures (CVE) naming convention.

References:
ARS: RA-5.CMS-1
NIST 800-42: Table 3.2
NIST 800-53: RA-5
PISP: 4.1.1.5

Related CSRs: 1.4.4, 1.9.4, 10.2.1

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be documentation available showing that business partner, management-initiated penetration testing was accomplished according to appropriate standards and procedures.

Protocols: 1. Examine organizational records or documents to determine if the organization scans for vulnerabilities in the information system on an organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported.
2. Examine the latest vulnerability scanning results to determine if the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans.
3. Examine the latest vulnerability scanning results to determine if patch and vulnerability management is handled in accordance with NIST SP 800-40 (Version 2).
4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the vulnerability scanning control is implemented.
5. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts vulnerability scanning of the information system on an ongoing basis.
6. Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the vulnerability scanning control are documented and the resulting information used to actively improve the control on a continuous basis.
7. Interview selected organizational personnel with risk assessment responsibilities to determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.
8. Examine previous vulnerability scan results to ensure that the tools used for vulnerability scanning include the capability to update the list of information system vulnerabilities scanned.
9. Examine organizational records or documents to determine if the organization updates the list of information system vulnerabilities scanned on an organization-defined frequency or when significant new vulnerabilities are identified and reported.
10. Examine organizational records or documents to determine if the organization provides adequate vulnerability scanning coverage including the key components of the information system (as defined by the organization) and the most up-to-date vulnerabilities.

10.9.2 Information concerning incidents and common vulnerabilities and threats is shared with FedCIRC, NIPC, owners of interconnected systems, other appropriate organizations, and local law enforcement when necessary. Automated mechanisms are employed to make security alert and advisory information available throughout the organization as needed.

References:
ARS: SI-5.1
HSPD-7: H(25)(b)
NIST 800-53: SI-5
PISP: 4.2.6.5

Related CSRs: 1.4.4, 1.6.1, 1.6.2, 1.6.6

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: There should be a process available for sharing security incidents and common vulnerabilities and threats with other the owners of interconnected systems, and federal and law enforcement authorities, when appropriate.

Protocols: 1. Examine organizational records or documents (including any logs documenting alerts/advisories) to determine if the organization: (i) receives information system security alerts and advisories; (ii) disseminates the alerts and advisories to appropriate personnel; (iii) takes appropriate actions in response; and (iv) documents the results including the date and time of each action taken.
2. Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization provides the capability to immediately react and respond to new security alerts and advisories.
3. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security alerts and advisories control is implemented.
4. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently receives and responds to security alerts and advisories for the information system on an ongoing basis.
5. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security alerts and advisories control are documented and the resulting information used to actively improve the control on a continuous basis.
6. Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization uses automated mechanisms to automatically disseminate security alerts and advisories to appropriate personnel and how the automated mechanisms are implemented.

Category: ***Network***

General Requirement

Control Technique

10.10 Logical controls shall be implemented over telecommunications access.

10.10.1 Communication software has been implemented to verify workstation identifications in order to restrict access through specific workstations: (1) verify UserIDs and passwords for access to specific applications; (2) control access through connections between systems and workstations; (3) restrict an application's use of network facilities; (4) protect sensitive data during transmission; (5) automatically disconnect at the end of a session; (6) maintain network activity records; (7) restrict access to tables that define network options, resources, and operator profiles; (8) allow only authorized users to shut down network components; (9) monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back to preauthorized phone numbers; (10) restrict in-house access to telecommunications software; (11) control changes to telecommunications software; (12) ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage and; (13) restrict and monitor access to telecommunications hardware or facilities.

References:
FISCAM: TAC-3.2.E.1

Related CSRs: 2.3.3, 2.8.5, 2.9.8, 2.9.9, 2.9.12, 2.9.19, 3.4.1, 3.6.2, 6.4.2, 10.5.1, 10.8.4

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Ensure that policies and procedures are in place that address all thirteen (13) of these points. If not, they should be developed in coordination with you company's IT department.

Protocols: 1. Review audit data confirming continuing operation of all specified features of the required software.
2. Review documentation confirming implementation of communications software having all of the required features.

Category: ***Network***

General Requirement

Control Technique

10.10 Logical controls shall be implemented over telecommunications access.

10.10.2 Remote and wireless access sessions are enabled through VPN links, using authorized VPN client software. FIPS-approved cryptography is used in combination with password authentication and certificate-based authentication to protect the confidentiality and integrity of remote sessions. All methods of remote access (e.g., dial-up, broadband) to the information system are authorized and monitored regularly, and each remote access method for the Medicare information system has been approved. Scans for unauthorized wireless access points are performed as needed but at least quarterly and appropriate action is taken if such access points are discovered.

References:

ARS: AC-17.2
ARS: AC-17.CMS-2
ARS: AC-18.1
NIST 800-53: AC-17
NIST 800-53: AC-18
PISP: 4.3.2.17
PISP: 4.3.2.18

Related CSRs: 3.6.3, 10.8.2, 10.8.9, 10.8.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Remote access should be controlled and there should be evidence of that control.

Protocols: 1. Examine organizational records or documents to determine if remote access is: (i) monitored on aperiodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs.
2. Examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; (ii) documents, monitors, and controls wireless access to the information system; and (iii) authorizes the use of wireless technologies.
3. Examine organizational records or documents to determine if the access control policy and procedures are consistent with NIST SP 800-48 and address usage, implementation, monitoring, and authorization of wireless technologies.
4. Examine organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures.
5. Examine organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials.
6. Examine the configuration of the information system to determine if controls are employed to restrict remote access to the system.
7. Examine organizational records or documents to determine if the organization tracks and monitors wireless access and usage in accordance with organizational policy and procedures.
8. Examine organizational records or documents to determine if wireless users have been authorized to access the information system.
9. Examine a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts.
10. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access and wireless access restriction controls are implemented.
11. Test the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions.
12. Test wireless access controls by attempting to access the information system through an unauthorized wireless connection to determine if the system is adequately protected from unauthorized wireless access.
13. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs remote access and wireless access restriction controls for the information system on an ongoing basis.
14. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access and wireless access restriction controls are documented and the resulting information used to actively improve the control on a continuous basis.
15. Examine organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods.
16. Examine organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures.
17. Examine the configuration of the information system to determine if wireless access to the system is only permitted through the use of authentication with encryption.
18. Test the wireless access restrictions by attempting to access the information system: (i) using an encrypted connection without authenticating to the system; and (ii) with a valid authentication mechanism over an unencrypted connection to determine if the access restrictions operate as intended.
19. Test the automated mechanism(s) within the information system to determine if each of the functions associated with the monitoring and control of remote access produce accurate and informative information, in accordance with remote access monitoring policy and procedures.
20. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.
21. Examine a remote access connection to the information system to determine if the connection requires the use of encryption and encryption is actually employed.
22. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization controls remote access through a managed access control point.
23. Test remote access controls by attempting to connect remotely to the information system without connecting through the managed access control point to determine if remote access can be achieved without following organizational policy and procedures.

Category: ***Network***

General Requirement

Control Technique

10.10 Logical controls shall be implemented over telecommunications access.

10.10.3 Secure management protocols are enabled through VPN link(s) if connected to a network, and remote administration is used. FIPS-approved encryption standards are used in combination with password authentication or additional authentication protection (e.g., token-based, biometric).

References:
ARS: AC-17.CMS-1
NIST 800-53: AC-17
PISP: 4.3.2.17

Related CSRs: 2.9.11, 10.8.2

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Remote administration should be carefully managed and controlled. Use of encryption features should be evaluated and approved by knowledgeable persons.

Protocols: 1. Examine organizational records or documents to determine if remote access is: (i) monitored on aperiodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs.
2. Examine organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures.
3. Examine organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials.
4. Examine the configuration of the information system to determine if controls are employed to restrict remote access to the system.
5. Examine a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented.
7. Test the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs remote access controls for the information system on an ongoing basis.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Examine organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods.
11. Examine organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures.
12. Test the automated mechanism(s) within the information system to determine if each of the functions associated with the monitoring and control of remote access produce accurate and informative information, in accordance with remote access monitoring policy and procedures.
13. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.
14. Examine a remote access connection to the information system to determine if the connection requires the use of encryption and encryption is actually employed.
15. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization controls remote access through a managed access control point.
16. Test remote access controls by attempting to connect remotely to the information system without connecting through the managed access control point to determine if remote access can be achieved without following organizational policy and procedures.

Category: ***Network***

General Requirement

Control Technique

10.10 Logical controls shall be implemented over telecommunications access.

10.10.4 Automated mechanisms are employed to facilitate the monitoring and control of remote access methods, and all remote access are controlled through a limited number of managed access control point. Remote access for privileged functions is permitted only for compelling operational needs and the rationale for such access is documented in the information system security plan.

References:

ARS: AC-17.1
ARS: AC-17.3
NIST 800-53: AC-17
PISP: 4.3.2.17

Related CSRs: 2.9.11, 10.8.2, 10.8.10

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). The organization permits remote access for privileged functions only for compelling operational needs. NIST SP 800-63 provides guidance on remote electronic authentication.

Protocols: 1. Examine organizational records or documents to determine if remote access is: (i) monitored on aperiodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs.
2. Examine organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures.
3. Examine organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials.
4. Examine the configuration of the information system to determine if controls are employed to restrict remote access to the system.
5. Examine a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts.
6. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented.
7. Test the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs remote access controls for the information system on an ongoing basis.
9. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access control are documented and the resulting information used to actively improve the control on a continuous basis.
10. Examine organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods.
11. Examine organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures.
12. Test the automated mechanism(s) within the information system to determine if each of the functions associated with the monitoring and control of remote access produce accurate and informative information, in accordance with remote access monitoring policy and procedures.
13. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.
14. Examine a remote access connection to the information system to determine if the connection requires the use of encryption and encryption is actually employed.
15. Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization controls remote access through a managed access control point.
16. Test remote access controls by attempting to connect remotely to the information system without connecting through the managed access control point to determine if remote access can be achieved without following organizational policy and procedures.

Category: ***Network***

General Requirement

Control Technique

10.10 Logical controls shall be implemented over telecommunications access.

10.10.5 For wireless devices, service set identifier broadcasting is disabled and the following wireless access controls are implemented: (1) encryption protection is enabled; (2) access points are placed in secure areas; (3) access points are shut down when not in use (i.e., nights, weekends); (4) a firewall is implemented between the wireless network and the wired infrastructure; (5) MAC address authentication is utilized; (6) static IP addresses, not DHCP, is utilized; (7) personal firewalls are utilized on all wireless clients; (8) file sharing is disabled on all wireless clients; (9) Intrusion detection agents are deployed on the wireless side of the firewall; and (10) wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

References:

ARS: AC-18.CMS-1
ARS: AC-18.CMS-2
CMS: Directed
NIST 800-53: AC-18
PISP: 4.3.2.18

Related CSRs: 1.13.8, 2.2.28, 10.8.11

Applicability: ABMAC, COB, CWF, DC, DMEMAC, EDC, PartA, PartB, PSC, SS

Guidance: NIST SP 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards. Data sent via wireless devices should be protected using encryption.

Protocols: 1. Examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; (ii) documents, monitors, and controls wireless access to the information system; and (iii) authorizes the use of wireless technologies.
2. Examine organizational records or documents to determine if the access control policy and procedures are consistent with NIST SP 800-48 and address usage, implementation, monitoring, and authorization of wireless technologies.
3. Examine organizational records or documents to determine if the organization tracks and monitors wireless access and usage in accordance with organizational policy and procedures.
4. Examine organizational records or documents to determine if wireless users have been authorized to access the information system.
5. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the wireless access restrictions control is implemented.
6. Test wireless access controls by attempting to access the information system through an unauthorized wireless connection to determine if the system is adequately protected from unauthorized wireless access.
7. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs wireless access restrictions an ongoing basis.
8. Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the wireless access restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.
9. Examine the configuration of the information system to determine if wireless access to the system is only permitted through the use of authentication with encryption.
10. Test the wireless access restrictions by attempting to access the information system: (i) using an encrypted connection without authenticating to the system; and (ii) with a valid authentication mechanism over an unencrypted connection to determine if the access restrictions operate as intended.