CMS Manual System

Pub 100-17 Medicare Business Partners Systems Security

Transmittal 5

Department of Health & Human Services

Center for Medicare and & Medicaid Services

Date: DECEMBER 23, 2004

Change Request # 3605

SUBJECT: Business Partners Systems Security Manual

I. SUMMARY OF CHANGES: The Manual is being updated to reflect changes to Federal laws, NIST guidance, CMS policies, standards, procedures and guidelines. Additionally, the Manual is being updated to inform Business Partners of security deliverables' due dates for FY 2005 and with minor grammatical changes.

NEW/REVISED MATERIAL :

EFFECTIVE DATE : October 1, 2004

IMPLEMENTATION DATE : February 28, 2005

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)

R = REVISED, N = NEW, D = DELETED – ***Only One Per Row.***

R/N/D	Chapter / Section / SubSection / Title
R	Table of Contents
R	1.0/ Introduction
R	2.0/2.1/ Consortium Contractor Management Officer and CMS Project Officer (CCM0/PO)
R	2.0/ 2.2/ The (Principal) Systems Security Officer (SSO)
R	2.0/ 2.5/ Personnel Security/Suitability
R	3.0/ IT Systems Security Program Management
R	3.0/ 3.1/ System Security Plan (SSP)
R	3.0/ 3.3/ Risk Assessment
R	3.0/ 3.4/ Information Technology Systems Contingency Plan

R	3.0/ 3.5/ 3.5.1/ Annual Compliance Audit
R	3.0/ 3.5/ 3.5.2/ Corrective Action Management Process and Plans of Action and Milestones
R	3.0/ 3.6/ 3.6.1/ Computer Security Incident Response
R	3.0/ 3.7/ Systems Security Profile
R	3.0/ 3.8/ Fraud Control
N	3.0/ 3.9/ Patch Management
N	3.0/ 3.10/ Security Management Resources
N	3.0/ 3.10/ 3.10.1/ Security Configuration Management
N	3.0/ 3.10/ 3.10.2/ National Institute of Standards and Technology (NIST)
R	4.0/ 4.1/ Information Security Levels
R	4.0/ 4.1/ 4.1.2/ 4.1.2.4/ Level 4: High Criticality and National Security Interest
R	4.0/ 4.2/ 4.2.2/ Security Room
R	4.0/ 4.2/ 4.2.6/ Intrusion Detection System (IDS)
R	5.0/ Internet Security
R	Appendix A/ 1.0/ CMS Core Security Requirements
R	Appendix A/ 2.0/ 2.1/ CSR Reponses
R	Appendix A/ 2.0/ 2.1/ 2.1.1/ All Responses
R	Appendix A/ 2.0/ 2.1/ 2.1.2/ Yes Responses
R	Appendix A/ 2.0/ 2.1/ 2.1.3/ No Responses
R	Appendix A/ 2.0/ 2.1/ 2.1.4/ Partial Responses
R	Appendix A/ 2.0/ 2.1/ 2.1.5/ Planned Responses
R	Appendix A/ 2.0/ 2.1/ 2.1.6/ N/A Responses
N	Appendix A/ 2.0/ 2.2/ Weaknesses
R	Appendix A/ Attachment A
R	Appendix B/ 4.0/ 4.2/ Coordination With Other Buesiness Partners
R	Appendix B/ 5.0/ Medicare IT Systems Contingency Plan
R	Appendix B/ 6.0/ 6.1/ Claims Processing Data Centers
R	Appendix B/ 6.0/ 6.5/ Test Planning
R	Appendix B/ 8.0/ 8.1/ Business Partner Management
R	Appendix B/ 12.0/ References
R	Appendix E/ Glossary

III. FUNDING:

No additional funding will be provided by CMS; Contractor activities are to be carried out within their FY 2005 operating budgets.

IV. ATTACHMENTS:

Business Requirements

Manual Instruction

Unless otherwise specified, the effective date is the date of service.

Attachment - Business Requirements

Pub. 100-17	Transmittal: 5	Date: December 23, 2004	Change Request 3605

SUBJECT: Business Partners Systems Security Manual (BPSSM)

I. GENERAL INFORMATION

A. Background: This change request will provide an update to sections of CR 3106.

B. Policy: Passage and publication of the Medicare Modernization Act of 2003 (Section 912), the Federal Information Security Management Act of 2002, NIST guidance and CMS policies, standards, guidelines and procedures.

C. Provider Education: None.

II. BUSINESS REQUIREMENTS

"Shall" denotes a mandatory requirement
"Should" denotes an optional requirement

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)								
		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
3605.1	Medicare contractors shall complete and submit security deliverables according to the scheduled outlined in the BPSSM.	X	X	X	X	X	X	X	X	
3605.2	Medicare contractors shall have patching and vulnerability policies and a documented process for handling patches.	X	X	X	X	X	X	X	X	
3605.3	Medicare contractors shall establish and maintain a configuration management program.	X	X	X	X	X	X	X	X	
3605.4	Medicare contractors shall utilize NIST and other guidance documents to develop security standards, templates and processes as part of their configuration management program.	X	X	X	X	X	X	X	X	

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)								
		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
3605.5	Medicare contractors shall complete and submit the CMS Tool Suite according to the instructions outlined in the BPSSM's Appendix A.	X	X	X	X	X	X	X	X	
3605.6	Medicare contractors shall implement the core security requirements found in the BPSSM's Attachment A.	X	X	X	X	X	X	X	X	

III. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions: N/A

X-Ref Requirement #	Instructions

B. Design Considerations: N/A

X-Ref Requirement #	Recommendation for Medicare System Requirements

C. Interfaces: N/A

D. Contractor Financial Reporting /Workload Impact: There will be no significant change, if any, on the contractors' workload.

E. Dependencies: This change request is not dependent upon another change request. Any change requests that are written in the future that relates to this change request will provide updates and/or clarification to systems security.

F. Testing Considerations: N/A

IV. SCHEDULE, CONTACTS, AND FUNDING

Effective Date*: October 1, 2004 **Implementation Date:** February 28, 2005 **Pre-Implementation Contact(s):** Sherwin Schulterbrandt, 410-786-0743 **Post-Implementation Contact(s):** Sherwin Schulterbrandt, 410-786-0743	**Medicare contractors shall implement these instructions within their current operating budgets.**

***Unless otherwise specified, the effective date is the date of service.**

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

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

(Rev.5 , December 23, 2004)

CMS/Business Partners

Systems Security Manual

Table of Contents (Rev. 5, 12-23-04)

Appendices

1.0 Introduction

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

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 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, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.

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 a system security program at a business partner site.
- Appendix A: CMS Core Security Requirements (CSRs) and the Contractor Security Assessment Tool (CAST), which provides the following:
  - An overview of the Core Security Requirements
  - An overview of the Contractor Assessment Security Tool (CAST).

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

- Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to provider of service.
- Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits.
- Public Law 93-579, The Privacy Act of 1974, as amended.
- Public Law 99-474, Computer Fraud & Abuse Act of 1986.
- Public Law 100-235, Computer Security Act of 1987.
- Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35.
- Public Law 104-106, Clinger-Cohen Act of 1996 (formerly called Information Technology Management Reform Act.
- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA), 1996.

http://aspe.os.dhhs.gov/admnsimp/index.shtml

- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996.
- Public Law 106-398, National Defense Authorization Fiscal Year 2001, Government Information Security Reform Act (GISRA) of 2000.
- Office of Management and Budget (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/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/index.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
- GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999.

  http://www.gao.gov/special.pubs/ai12.19.6.pdf
- CMS System Security Plans (SSP) Methodology, Draft Version 3.0, *November 6*, 2002.

  http://www.cms.hhs.gov/it/security/docs/ssp_meth.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
- *Federal Information Security Management Act of 2002 (FISMA), November 27, 2002.*

  http://csrc.nist.gov/policies/FISMA-final.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

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

- Department of Health and Human Services, Automated Information Systems Security Program Handbook (DHHS AISSP).
  http://wwwoirm.nih.gov/policy/aissp.html
- NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC), November 1991.
  http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, SP800-12.
  http://csrc.nist.gov/publications/nistpubs/800-12
- Code of Federal Regulations, Regulation 36 CFR Part 1228 Subpart K, NARA36
  http://www.access.gpo.gov/nara/cfr/cfrhtml_00/Title_36/36cfr1228_00.html
- Code of Federal Regulations, Regulation 5 CFR Part 731 – Suitability, 5CFR731
  http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html
- FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25 U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, PUB46-3.
  http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- CMS Internet Security Policy
  http://www.cms.hhs.gov/it/security/References/ps.asp
- CMS Information Security Risk Assessment (RA) Methodology, Version # 1.1 September 12, 2002.
  http://www.cms.hhs.gov/it/security/References/ps.asp
- *Homeland Security Presidential Directive/HSPD-7*
  http://www.fas.org/irp/offdocs/nspd/hspd-7.html.
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, Security Self Assessment Guide for Information Technology Systems, November 2001.*
  http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
- *CMS Information Security Acceptable Risk Safeguards (ARS) Version 1.2, October 25, 2004.*
  http://www.cms.hhs.gov/it/security

CMS Core Security Requirements will be updated periodically to reflect changes in these or other applicable documents.

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

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

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 Project Officers (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 systems security plans and reports including security incident reports.
- Provide the personnel and technical assistance necessary to respond to CMS security policies and procedures.

2.2 The (Principal) Systems Security Officer (SSO)

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

Business partners must designate a Systems Security Officer (SSO) qualified to manage the Medicare system security program and assure 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. A qualified SSO that 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 to ensure implementation and maintenance of effective security controls. The SSO position in each contractor should be a full-time position staffed with an individual fully qualified, and preferably credentialed, in systems security. 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. 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 they must coordinate security actions through the principal SSO for Medicare records and operations. The SSO assures compliance with CMS Core Security Requirements by performing the following:

- Facilitating the Medicare IT system security program and assuring necessary safeguards are in place and working.
- Coordinating system security activities throughout the organization.
- Ensuring that IT systems security requirements are considered during budget development and execution.
- Reviewing compliance of all components with the CMS Core Security Requirements and reporting vulnerabilities to management.
- Establishing an incident response capability, investigating systems security breaches, and reporting significant problems (see Section 3.6) to business partner management, and CMS.
- 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 RFPs and subcontracts involving the handling, processing, and analyzing of Medicare data.
- Maintaining systems security documentation in the Systems Security Profile for review by CMS and external auditors.

- Cooperating in all official external evaluations of the business partner's systems security program.
- Facilitating the completion of the Risk Assessment (see Section 3.2).
- Ensuring that an operational Information Technology Systems Contingency Plan is in place and tested (see Section 3.4).
- Documenting and updating the Corrective Action *Management Process* (see Section 3.5). Updates follow issuance of new requirements, risk assessment, internal audit, external evaluation, and, of course, the target dates themselves. (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 Systems Security Officer should earn 40 hours of continuing professional education credits from a recognized national information systems security organization each year. The educational sessions at the security best practices conference can be used to towards fulfilling CMS business partners continuing education credits. The qualifying sessions and associated credit hours will be noted on the best practices conference agenda.

2.5 Personnel Security/Suitability

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

CMS is currently reviewing business partner position security and personnel investigative requirements. The results of this review will be published when completed. In the interim, CMS is publishing the following minimum investigative requirement for all prospective business partner and contractor employees requiring access to CMS sensitive information. A contractor also can be a subcontractor to a CMS business partner.

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 is not merely based on position or title and favorable results from a background check. This 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. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

Business partners must *have policies and* procedures, *and implement controls* or plans that fulfill the CMS Core Security Requirements (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 fully implemented when policies and procedures are communicated to individuals who are required to follow them. 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.

Understand that meeting requirements does not validate the quality of the program. Managers with oversight responsibility must understand the processes and methodology behind the requirements. The following Table 3.1 identifies key requirements and provides high-level descriptions of them. As appropriate, this section 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 CMS Core Security Requirements. The supporting documentation, planned safeguards, and related schedules must be recorded using the Contractor Assessment Security Tool (CAST*, s*ee Appendix *A*). To perform the self-assessment, business partners must conduct a systematic review of the Core Security Requirements using *the* CAST. *The* CAST provides a self-assessment form that includes audit protocols to assist in the review of the requirements.

The CMS Core Security Requirements include key security-related tasks. Table 3.1 indicates when or how often these tasks need to be rechecked, 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 of 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.

Table 3.1. Planning Table

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
Appendix A, Section 2, Self-Assessment using *the* CAST	Each Federal fiscal year	CCMO/PO with a copy to CMS CO. Systems Security Profile	See Appendix A, Section 2, for an overview of *the* CAST. Self-assessment results recorded using *the* CAST are to be discussed in the Certification Package.	☐
3.1 System Security Plans	*For each GSS and MA, the SSP must be reviewed, updated, and certified by management each Federal fiscal year (minimum), or upon significant change.*	Systems Security Profile SSO CMS CO	*System Security Plans are to be reviewed, updated, and certified by management—and indicated as such in both the Certification Package/statement of certification and the Systems Security Profile.* More information about System Security Planning can be found in the CMS SSP Methodology.	☐
3.2 Risk Assessment (Report)	*For each GSS and MA, the Risk Assessment must be reviewed, updated, and certified by management each Federal fiscal year (minimum), or upon significant change.*	Systems Security Profile CMS CO	*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 Systems Security Profile.* The Risk Assessment Report is an attachment *to* the System Security Plan. More information about Risk Assessment Reports can be found in the CMS Information Security RA Methodology.	☐

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.3 Certification	Each Federal fiscal year	CCMO/PO with a copy to CMS CO.	Fiscal intermediaries and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (*I*nternal *C*ontrols) 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 project officers.	☐

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.4 Information Technology Systems Contingency Plan	*Contingency Plans must be reviewed, updated, and certified by management each Federal fiscal year (minimum), or upon significant change.* Plans must be tested annually.	Systems Security Profile SSO CMS CO	Management and the SSO must approve the Plan. *The IT 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 Systems Security Profile.* More information about contingency planning can be found in *An Introduction to Computer Security: The NIST Handbook. Special Pub 800-12*, and the *Contingency Planning Guide for Information Technology Systems: NIST Special Pub 800-34*.	☐

3.5 Compliance	Each Federal Fiscal year	CCMO/PO Systems Security Profile SSO CMS CO May be stored as paper documents, electronic documents, or a combination.	There are two (2) components to compliance: (1) **Annual Compliance Audit** *(ACA)*: Once a year, an independent audit will be performed on four (4) categories of the CMS Core Security Requirements *(CSRs)* to validate the self-assessment. CMS will determine the four categories the audit will validate *and inform the business partners via the BPSSM*. **(2) Corrective Action *Management Process*** *The* Corrective Action *Management Process* addresses findings of annual system security assessments including the *ACA*, *the annual CMS Self Assessment* Review, SAS 70 audits (if any), CFO controls audits (if any), Section 912 evaluation (if applicable), and Data Center tests and reviews (if applicable).	
3.6 Incident Reporting and Response	As necessary	CCMO/PO Systems Security Profile	The HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file in the Security Organization.		

LEGEND:

Contractor Assessment Security Tool	CAST
Central Office (CMS)	CO
Consortium Contractor Management Officer	CCMO
Project Officer (CMS)	PO
Senior Information Systems Security Officer	CMS SISSO
Business Partner Systems Security Officer	SSO
General Support System	GSS
Major Application	MA

When submitting documentation to CCMOs or CMS Central Office, use Federal Express, certified mail, or the equivalent (receipt required). *For supporting documentation (such as Risk Assessments, Contingency Plans, Systems 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:

- CMS CO

Security and Standards Group
Mail Stop- N2-14- 26
7500 Security Blvd.
Baltimore, MD 21244-1850

The following are the contacts and addresses of 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
404-562-7250

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

The objective of an Information Security (IS) 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, Computer Security Act of 1987. All Medicare claims-related applications and systems must be covered by SSPs if they are categorized as a Major Application (MA)[1] or General Support System (GSS)[2].

The purpose of the SSP is to provide an overview of the security requirements of the 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 system security profiles. 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 forms the primary reference documentation for testing and evaluation, whether by CMS, the 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 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.

---

[1] Major Application–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 business-related function.

[2] General Support System–An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people. It provides support for a variety of users and/or applications. Individual applications supporting different business-related functions may run on a single GSS. Users may be from the same or different organizations.

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 which is available on the CMS *W*eb 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 which is also available at the same *W*eb 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 if 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 must be placed in the Medicare Contractor's System Security Profile. The updated SSP must be placed in the Medicare Contractor's System Security Profile and a copy must be provided to the CMS Central Office.

Contractors given direction to update their current SSP(s) to include front-end, back-end, and/or other claims processing systems must use 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 input claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to the following systems: 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 the following systems: 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 including the ORIGINAL signed, dated CMS SSP certification form must be sent to the CMS Central Office (Security and Standards Group/Mail Stop N2-14-26/7500 Security Blvd./Baltimore, MD 21244-1850). These documents must be received by CMS *on CD-ROM* ten (10) working days after they have been developed, updated, or *re-certified, and the 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 copy*. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

In summary, your SSP must be updated annually and certified unless there are changes to either as discussed above that would necessitate a more frequent update.

Should you require SSP technical assistance, direct your questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/*Northrop Grumman IT* Help Desk at (703) 620-8585.

3.2 Risk Assessment

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

Business partners are **required** to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology. This methodology is available at the following CMS *W*eb site: *http://www.cms.hhs.gov/it/security/default.asp*.

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 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[3] 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 Risk Assessment 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 an attachment to the SSP must be sent to the CMS Central Office (Security and Standards Group; Mail Stop N2-14-26; 7500 Security Blvd.; Baltimore, MD 21244-1850). These documents must be received by CMS *on CD-ROM* ten (10) working days after they have been developed, updated, or *re-certified, and a statement of certification for the Risk Assessment must be submitted in hard copy along*

---

[3] The National Institute of Standards and Technology defines "significant change to an information systems is 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."

with the electronic copy. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

In summary, your RA must be updated annually and certified unless there are changes to either as discussed above that would necessitate a more frequent update.

Should you require RA technical assistance, direct your questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/*Northrop Grumman IT* Help Desk at (703) 620-8585.

Business *p*artners should refer to the Acceptable Risk Safeguards document to aid in the preparation of a risk assessment. This document can be found at *http://www.cms.hhs.gov/it/security/References/ps.asp*.

3.3 Certification

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

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 Core Security Requirements. 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 Project Officer*. 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 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 and CMS Information Security RA Methodology)
- Information Technology Systems Contingency Plan (see Section 3.4 and Appendix B)
- Results of *the ACA* (see Section 3.5)
- Corrective Action *Management Process* (see Section 3.5).

3.4 Information Technology Systems Contingency Plan

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

All business partners are required to develop and document an Information Technology 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 Information Technology 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 make sure 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 Information Technology Systems Contingency Plans. See Item 3.4 in Table 3.1, *Section 3.0,* for other references.

Medicare Contractors must review their 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 your System Security Profile. Business partner's management and the system security officer (SSO) must approve newly developed or updated IT Systems Contingency Plans. Information on Medicare IT systems contingency planning can be found in Appendix B of the BPSSM.

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*. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

3.5.1 Annual Compliance Audit (ACA)

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

Each business partner must conduct an Annual Compliance Audit *(ACA)* on four (4) out of the ten (10) categories of the CMS Core Security Requirements. *See Appendix A, Section 1.0 for a description of the 10 categories of CMS Core Security Requirements.* A compliance audit is a performance review of a business partner's systems security program that tests whether the systems security controls comply with CMS' CSRs (*Attachment* A of this manual) and are implemented properly. The audit will be documented through an *ACA* Report.

Government auditing standards dictate business partner staff assigned to conduct an audit should possess adequate professional proficiency for the tasks required[4]. An audit team should include audit skills and familiarity with implementation of the physical and IT security features utilized by the business partner or required by CMS. Required audit skills include proficiency in basic auditing tasks, communicating, and project management. An internal audit department with these qualifications may perform the *ACA*.

An *ACA* will have a verifiable information system security auditor assigned to coordinate the interviews, tests, and analysis, and provide approval of the final report. The information systems auditor must be independent of the organization directly responsible for design, operation, and/or management of the systems being audited.

The *ACA r*eport must include the following:

1. A Summary of Controls: These controls are those instructions that the business partner has implemented to comply with the CMS CSRs. The summary of controls should be derived from the source documentation referenced in the Contractor Assessment Security Tool (CAST).

2. A Description of Review Procedures and Tests: This description must include procedures and tests performed by the organization (internal or external) performing the *ACA* as well as a description of the results of such tests.

A CMS directed SAS 70 and/or OIG CFO *E*DP audit will meet the requirement of the identified CSR categories for the *ACA* if either audit was performed during the current fiscal year and addressed the categories identified by CMS for the current fiscal year. An *ACA* must be performed for those categories that are not covered by a SAS 70 or OIG CFO *E*DP audit.

The *ACA* must be completed by September 30, *2005*. The categories of the CMS Core Security Requirements (CSR) to be audited in fiscal year *2005* are: *(1) Entity-wide security program planning and management, (2) Application software development and change control, (3) Access control, and (4) System software.*

---

[4] Government Auditing Standards: 1994 Revision (GAO/OCG-94-4, Paragraphs 3.3 – 3.5 and 3.10.)

Medicare contractors who received Section 912 evaluations or Data Center system tests and evaluations in FY04 or FY05 do not need to conduct an ACA for FY05. Those entities who are notified of gaps, weaknesses, and/or findings should focus on remediating the identified issues in lieu of conducting an ACA. All Medicare contractors who did not receive Section 912 evaluations or Data Center system tests and evaluations must conduct an ACA.

A copy of the completed ACA must be submitted on CD-ROM to the CMS Central Office, your CCMO for Title XVIII contracts, or the PO for FAR contracts by October 17, 2005. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used. A copy must also be placed in the Systems Security Profile.

CMS recommends *that* the ACA report be organized by subject matter to facilitate ease of review and use. The categories should include (1) CAST CSR *c*ategories, *(2)* OIG CFO EDP audit, (*3*) SAS 70 review, and*/or* (*4*) *any other open findings from independent or external audits or reviews*.

3.5.2 Corrective Action Management Process and Plans of Action and Milestones

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

Another component of compliance requires the preparation of *remediation plans*. *Remediation plans must be in POA&M format and must be prepared and submitted as directed by the OIS/SSG.* Medicare business partners must review their security compliance and determine the degree of compliance. *CMS requires* the timely preparation and submission of *remediation plans to correct known deficiencies in information security.*

Remediation plans for the ACA must be prepared and submitted in POA&M format along with the ACA Report within ten (10) working days after the completion of the ACA for any noted deficiencies. A status of scheduled implementation actions must be included to ensure that approved safeguards are in place or in process. When an item in the plan is a major risk, feedback will be provided by CMS within ninety (90) days of submission.

Remediation plans for all other IT/electronic data processing reviews, audits, assessments, and evaluations must be in POA&M format and submitted to the OIS/SSG according to the schedule provided by CMS.

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[5]. Additionally, periodic "Plans of Action and Milestones" (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[6]. This reporting requirement applies to a broader scope of security weaknesses, as they are not limited to weaknesses identified by specific audits and reviews (such as those covered under The Federal Managers Financial Integrity Act of 1982). In the case of FISMA, any security weakness[7] identified for covered systems must be reported and included in a periodic POA&M report.

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" implemented requirements for annual evaluation, testing, and reporting on security programs at "Medicare Administrative Contractors" (MACs) as well as existing Carrier and Intermediary business partners (to include their respective Data Centers). These "Section 912" evaluations and reports require an annual on-site review of business

---

[5] FISMA Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires that each agency provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."

[6] POA&M instructions for Federal agencies are described in OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act.

[7] Weaknesses are defined as those vulnerabilities that require corrective action (CMS Plan of Action and Milestones (POA&M) Guide – June 22, 2004 – 2nd Draft)

partner security programs to ensure that the business partner security programs meet the requirements for information security imposed on Federal agencies under FISMA. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies be addressed in a report that must 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 overall effect of the Section 912 legislation is to definitively pass the requirements of FISMA down to Medicare business partners and implement a requirement for annual Section 912 evaluations.

As a result of FISMA and Section 912, business partners will undergo annual independent evaluations (initiated and coordinated by the OIS/SSG). Business partners shall prepare an initial plan for remediating weakness (in accordance with the approved POA&M format), containing weaknesses identified during the evaluations, along with associated action plans, within 45 days of receipt of the results of the final evaluation report.

On a quarterly basis, business partners shall prepare a similar report (in accordance with the approved POA&M format) that provides updates on progress towards completion of remediation efforts for weaknesses identified from all known sources. Both the initial and quarterly POA&M reports will contain the following data:

- *Weakness Identifier. Will be used to track and correlate weaknesses that are ongoing throughout quarterly submissions to CMS.*
- *Weakness. Any program or system-level information security vulnerability that poses an unacceptable risk to the confidentiality, integrity, or availability of CMS sensitive information.*
- *Point of Contact (POC). The organization or title of the position within the entity that is responsible for mitigation of the weakness.*
- *Resources required. The funding or man-hours necessary for mitigating the weakness. The type of funding (current, new, or reallocated) should be noted.*
- *Scheduled Completion Date. Completion Dates should be set based on a realistic estimate of the amount of time it will take to collect the resources for the corrective action and implement/test the corrective action.*
- *Milestones with Completion Dates. Outlines the specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step.*
- *Changes to Milestones. Indicates the new estimated future date of a milestone's completion if the original date is not met.*
- *Identified in CFO Audit or other review. Indicates the review type, reviewing organization that identified the weakness, and the date on which the weakness was logged (i.e., audit date).*
- *Status. Indicates the stage or state of the weakness corrective action (Completed, Ongoing, or Delayed).*

- *Comments. Used for additional detail or clarification; must be used if there is a delay.*
- *Risk Level. A ranking that determines the impact of a vulnerability to the system, data, and/or program.*

The contractor security tool suite is designed to accurately maintain the data associated with the above-listed weakness and findings sources, and generate an appropriate, up-to-date POA&M report. Additionally, the Tool Suite will also produce an appropriate database submission for inclusion in the POA&M report submittal package. After initial submission of a POA&M report, Medicare contractors must submit quarterly a copy of the completed POA&M (as well as the submittal database) on CD-ROM to the CMS Central Office and your CCMO (for Title XVIII and MAC contracts) or PO (for FAR contracts). The quarterly submission schedule is no later than January 15, April 15, July 15, and October 15 of each year. Please be advised that this information should not be submitted via unsecured email. Registered mail or its equivalent should be used. A copy must also be placed in the System Security Profile.

3.6.1 Computer Security Incident Response

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

If a violation of the law is suspected, CMS will notify the Office of the Inspector General's Computer Crime Unit and submit a report to the FedCIRC of the incident with a copy to the CMS Senior Information Systems Security Office.

All confirmed incidents are considered major risks and must be reported immediately to the CCMO/PO. The CCMO/PO should be kept informed of the status of the incident follow-up until the incident is resolved. CCMOs/POs should be provided with a point of contact at the Medicare contractor's site for the security incident. The phone numbers for the CCMOs can be found in the contact address list in Section 3, above.

Business partners should also contact the CMS Service Desk (410-786-2580) and report any confirmed security incident. 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/need-to-know basis. When other entities would be notified of incidents at external business partner sites, CMS would coordinate with legal and public affairs contacts at the effected entities.

Business *p*artners should refer to The CMS System Security Incident Handling Procedures for further guidance. This document can be found at *http://www.cms.hhs.gov/it/security/References/ps.asp*.

3.7 System Security Profile

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

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

- Risk Assessment
- Completed CAST Self Assessment(s)
- *ACA* Report
- Information Technology Systems Contingency Plans
- Security reviews undertaken by DHHS OIG, CMS, IRS, GAO, consultants, subcontractors, and business partner security staff
- Corrective Action Management Process for each security review
- System Security Plan (for each GSS and MA)
- Systems security policies and procedures.

Secure the profile, keep it up-to-date, and maintain pointers to other relevant documents. Require secure off-site storage of a backup copy of the System Security Profile preferably at the site where back-up tapes and/or back-up facilities are located. Keep this back-up copy of the profile up-to-date, particularly the contingency plan report.

3.8 Fraud Control

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

Business partners are required to safeguard systems against fraud. The CMS Core Security Requirements 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, CMS Core Security Requirements and the Contractor Assessment Security Tool (CAST), and Appendix C, An Approach to Fraud Control.

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

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. 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.

NIST SP 800-40, "Procedures for Handling Security Patches," provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS does not normally require the verbatim use of NIST publications for the configuration of Medicare systems. However, 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. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

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 provides these and other guidelines and checklists at http://csrc.nist.gov/pcig/cig.html.

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 free of charge to the Internet community at http://www.cisecurity.com/benchmarks.html.

CMS does not require the verbatim use of these 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.

Table 3.2 contains links to security configuration guidelines and checklists for some of the more common systems 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. However, CMS highly encourages business partners to review and incorporate these concepts into the Medicare configuration management philosophy within their systems management and security programs.

Table 3.2. Configuration Guidelines

System Type	Standards and Checklists Available	Comments
UNIX / Solaris	*http://www.sun.com/solutions/blueprints/*	*Sun site for white papers (blueprints) on security and other Solaris topics.*
	http://sunsolve.sun.com	*Sun site for patches and security fixes.*

System Type	Standards and Checklists Available	Comments
	http://www.cisecurity.com/bench_solaris.html	Center for Internet security (CIS offshoot of SANS) site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
	http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	Defense Information Systems Agency (DISA) Unix configuration guidelines. Contains information for general UNIX security and specifications for Solaris.
UNIX / AIX	http://publib-b.boulder.ibm.com/redbooks.nsf/redbookabstracts/sg246066.html?open	IBM Redbooks on AIX Security.
	http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	DISA UNIX configuration guidelines. Contains information for general UNIX security and specifications for AIX.
UNIX / LINUX	http://www.cisecurity.com/bench_linux.html	CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
	http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	DISA UNIX configuration guidelines. Contains information for general UNIX security and specifications for LINUX.
	http://www.nsa.gov/selinux/index.html	NSA's Information Assurance Research Group developed guidelines and tools to implement LINUX for use in an environment with security requirements.
UNIX / HP-UX	http://www.cisecurity.com/bench_hpux.html	CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
	http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	DISA UNIX configuration guidelines. Contains information for general UNIX security and specifications for HP-UX.
Windows 2003 Windows XP Windows 2000 Windows NT 4.0 SQL Server IIS	1. http://www.microsoft.com/technet/Security/default.mspx 2. http://www.microsoft.com/technet/security/tools/mbsahome.mspx	Microsoft Security Site and a link to the Microsoft Baseline Security Analyzer (MBSA). MBSA includes a graphical and command line interface that can perform local or remote scans of Windows operating systems. MBSA runs on: Windows 2000, Windows XP, and Windows Server 2003 systems. MBSA will scan for common system misconfigurations in the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS), SQL Server, Internet Explorer, and Office. MBSA will also scan for missing security updates for the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, IIS, SQL Server, Internet Explorer, Office, Exchange Server, Windows Media Player, Microsoft Data Access Components (MDAC), MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, and Host Integration Server.
Windows XP	1. http://csrc.nist.gov/pcig/STIGs/WindowsXP.doc 2. http://csrc.nist.gov/pcig/CHECKLISTS/winxp-checklist-062504.zip	1. DISA Windows XP Security Technical Implementation Guide (STIG). 2. DISA Windows XP Checklist.
	http://www.cisecurity.com/bench_win2000.html	CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.

System Type	Standards and Checklists Available	Comments
	http://csrc.nist.gov/itsec/guidance_WinXP.html	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist - Special Publication 800-68 (Draft)
Windows 2000 Windows NT	http://www.cisecurity.com/bench_win2000.html	CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
Windows 2003 Windows XP Windows 2000 Windows NT 4.0	http://www.nsa.gov/snac/downloads_all.cfm	National Security Agency (NSA) guidelines for Windows security developed by NSA's Systems and Network Attack Center (SNAC)
Novell	http://www.novell.com http://developer.novell.com/research/appnotes/2000/june/03/a000603.htm http://developer.novell.com/research/appnotes/1997/november/06/04.htm	Novell Web site. The developer.novell.com site contains white papers and technical guidelines for security in Novell products.
	http://novell.unc.edu/security/security.htm	University of North Carolina security guideline
Oracle Database	http://www.oracle.com/solutions/security/index.html	Oracle's Web site for security in oracle products.
	http://www.cisecurity.com/bench_oracle.html	CIS site for system vulnerability assessment and configuration guidelines. Includes technical information on Oracle security configurations.
	http://csrc.nist.gov/pcig/STIGs/DATABASE-STIG-V7R0-DRAFT.zip	DISA Database configuration guideline, checklist, and STIG.
	http://www.nsa.gov/snac/downloads_all.cfm	National Security Agency (NSA) guidelines for Oracle security developed by NSA's Systems and Network Attack Center (SNAC)
Cisco Router	http://www.cisco.com	CISCO Web site.
	http://www.nsa.gov/snac/downloads_all.cfm	National Security Agency (NSA) guidelines for Cisco security developed by NSA's Systems and Network Attack Center (SNAC)
	http://www.cisecurity.com/bench_cisco.html	CIS site for system vulnerability assessment and configuration guidelines. Includes technical information on Oracle security configurations.
Juniper Router	http://csrc.nist.gov/pcig/CHECKLISTS/juniperrouterchecklistv5r2_1-062504.doc	DISA STIG for Juniper routers.
OS/390 and MVS	1. http://csrc.nist.gov/pcig/STIGs/os390-lparstig-v2r1-jul03.doc 2. http://csrc.nist.gov/pcig/CHECKLISTS/lpar-checklist-2v103-062504.doc 3. http://csrc.nist.gov/pcig/STIGs/OS-390V5R0-Vol1.zip 4. http://csrc.nist.gov/pcig/STIGs/OS-390V5R0-Vol2.zip 5. http://csrc.nist.gov/pcig/CHECKLISTS/OS390-racf-checklist-v4r13.doc 6. http://csrc.nist.gov/pcig/CHECKLISTS/OS390-acf2-checklist-v4r13.doc 7. http://csrc.nist.gov/pcig/CHECKLISTS/os390-tss-checklist-v4r13.doc	1. DISA OS/390 Logical Partition STIG 2. DISA OS/390 Logical Partition Checklist 3. DISA OS/390 MVS STIG Volume 1 4. DISA OS/390 MVS STIG Volume 2 5. DISA OS/390 RACF Checklist 6. DISA OS/390 ACF2 Checklist 7. DISA OS/390 TSS Checklist
VMS VAX	http://csrc.nist.gov/pcig/CHECKLISTS/vms-openvs-srrchklst-v2r11.zip	DISA VMS VAX Checklist

System Type	Standards and Checklists Available	Comments
Wireless security	1. *http://csrc.nist.gov/pcig/STIGs/Wireless-STIG-V3R1.zip* 2. *http://csrc.nist.gov/pcig/CHECKLISTS/wireless-chklstv2r11-073003.doc*	1. *DISA Wireless STIG* 2. *DISA Wireless Checklist*

3.10.2 National Institute of Standards and Technology (NIST) (Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

CMS, as a government agency, highly encourages business partners to review and incorporate the National Institute of Standards and Technology (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 information technology security issues. The publications are issued as Federal Information Processing Standards Publications (FIPS), Special Publications (SP), NIST Interagency Reports (NISTIRs), and Information Technology Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-XX) present documents of general interest to the computer security community. Federal Information Processing Standards Publications (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 the Federal Information Security Management Act (FISMA) of 2002, 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 publications for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are incorporated into the business partner 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 3.3 contains a listing of NIST publications relevant to common systems or technology utilized within the Medicare business partner community. Table 3.3 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 3.3. NIST Publications

Publication Number	Title
SP 800-72 (Draft)	*Guidelines on PDA Forensics*
SP 800-70 (Draft)	*The NIST Security Configuration Checklists Program*
SP 800-68 (Draft)	*Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*

Publication Number	Title
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66 (Draft)	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65 (Draft)	Integrating Security into the Capital Planning and Investment Control Process
SP 800-64	Security Considerations in the Information System Development Life Cycle
SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
SP 800-61	Computer Security Incident Handling Guide
SP 800-60	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 (Draft)	Security Considerations for Voice Over IP Systems
SP 800-57 (Draft)	Recommendation on Key Management
SP 800-56 (Draft)	Recommendation on Key Management
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53 (Draft)	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 Information Technology 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 Information Technology 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	Procedures for Handling Security Patches
SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques
SP 800-38B (Draft)	Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
SP 800-36	Guide to Selecting Information Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-33	Underlying Technical Models for Information Technology 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 Information Technology 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 Information Technology Security (A Baseline for Achieving Security)
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-25	Federal Agency Use of Public Key Technology 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	Guideline for Implementing Cryptography in the Federal Government

Publication Number	Title
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	Guide for Developing Security Plans for Information Technology Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC)
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook
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 Local Area Network 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)
FIPS 171	Key Management Using ANSI X9.17
FIPS 140-1	Security Requirements for Cryptographic Modules
FIPS 113	Computer Data Authentication
FIPS 112	Password Usage (part 1)
FIPS 102	Guidelines for Computer Security Certification and Accreditation
FIPS 87	Guidelines for EDP Contingency Planning
FIPS 83	Guideline on User Authentication Techniques for Computer Network Access Control
FIPS 81	DES Modes of Operation (includes Change Notice 1)
FIPS 74	Guidelines for Implementing and Using the NBS Data Encryption Standard Part 1 of 3
FIPS 73	Guidelines for Security of Computer Applications
FIPS 48	Guidelines on Evaluation of Techniques for Automated Personal Identification
FIPS 46-3	Data Encryption Standard (DES); specifies the use of Triple DES
FIPS 31	Guidelines for Automatic Data Processing Physical Security and Risk Management

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.

4.1 Information Security Levels

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

The security level designations within the CMS Business Partner Security Program are based on the following:

- The sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse).
- The operational criticality of data processing capabilities (i.e., the ramifications if data processing capabilities were interrupted for a period of time or subject to fraud or abuse).

There are four security level designations for data sensitivity and four security level designations for operational criticality. These security levels are summarized in Table 4.1 and described in more detail later in this *section*.

Table 4.1. Summary of Sensitivity and Criticality Levels

Level	Sensitivity	Criticality
1	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.	Systems requiring minimal protection. In the event of alteration or failure, it would have a minimal impact or could be replaced with minimal staff time or expense. This includes data that has low or no sensitivity.
2	Data has importance to CMS and 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.	Systems that are important but not critical to the internal management of CMS. If systems fail to function for an extended period of time, it would not have a critical impact on the organizations they support. This includes data that has moderate sensitivity.
3	The most sensitive unclassified data processed within CMS IT systems. This data requires the greatest number and most stringent information security safeguards at the user level.	Systems that are critical to CMS. This includes systems whose failure to function for even a short period of time could have a severe impact or has a high potential for fraud, waste, or abuse. This includes data that has high sensitivity.

Level	Sensitivity	Criticality
4	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. (CMS currently processes no information in this category.)	Systems are critical to the *well being* of CMS such as systems that handle sensitive but unclassified information, the loss of which could adversely affect national security interests. These systems must be protected in proportion to the threat of compromise or exploitation and the associated potential damage.

The appropriate business partner System Owner/Manager and System Maintainer/Developer must consider each system from both points of view, then choose the higher rating for the overall security level designation.

An MA or GSS may be compartmentalized, such that a given data set or sub-process is more sensitive than other data sets or sub-processes. The appropriate business partner System Owner/Manager and System Maintainer/Developer must assign the highest security level designation of any data set or sub-process within the system for the overall security level designation. This practice supports the following:

- **Confidentiality**. The system contains information that requires protection from unauthorized disclosure.
- **Integrity**. The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including the detection of such activities.
- **Availability**. The system contains information or provides services that must be available on timely basis to meet mission requirements or to avoid substantial losses.

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.

4.1.2.4 Level 4: High Criticality and National Security Interest
(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

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.

4.2.2 Security Room

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

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 (see 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.

4.2.6 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 *en*sure confidentiality, integrity, and availability of data moved over the Internet and will reconsider its policy at the appropriate time.

Appendix A:
CMS Core Security Requirements and the Contractor Assessment Security Tool (CAST)

Table of Contents

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

1.0 CMS Core Security Requirements

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

CMS Core Security Requirements *(CSRs)* detail technical requirements for business partners who use IT systems to process Medicare data. Business partners must establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data.

The Contractor Assessment Security Tool (CAST) will assist business partners in performing required annual systems security *self-assessments* and will also allow them to prepare for periodic audits by agencies, such as the Government Accounting Office (GAO), Internal Revenue Service (IRS), and Department of Health and Human Services (DHHS) Office of Inspector General (OIG), and CMS.

The CMS *CSRs* were 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-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/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
- 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 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001.*

  http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
- CMS System Security Plans (SSP) Methodology Draft Version 3.0, October 28, 2002.

  http://www.cms.hhs.gov/it/security/References/ps.asp
- *CMS Information Security Acceptable Risk Safeguards (ARS) Version 1.2, October 25, 2004.*

  http://www.cms.hhs.gov/it/security/References/ps.asp

- IRS 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), 1996.
  http://aspe.os.dhhs.gov/admnsimp/pl104191.htm
  http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm

CMS has organized the *CSRs* into Categories, General Requirements, Control Techniques, and Protocols. 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 Elements	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 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.
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.
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.
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

Category	Description
	and corrected.
Networks	These controls address the network*(s)* structure. The network structure must be protected and the data transmitted on the networks must be protected.

Each category is further organized into General Requirements, Control Techniques, and Protocols. Figure A-1 below shows the relationship among General Requirements, Control Techniques, and Protocols.

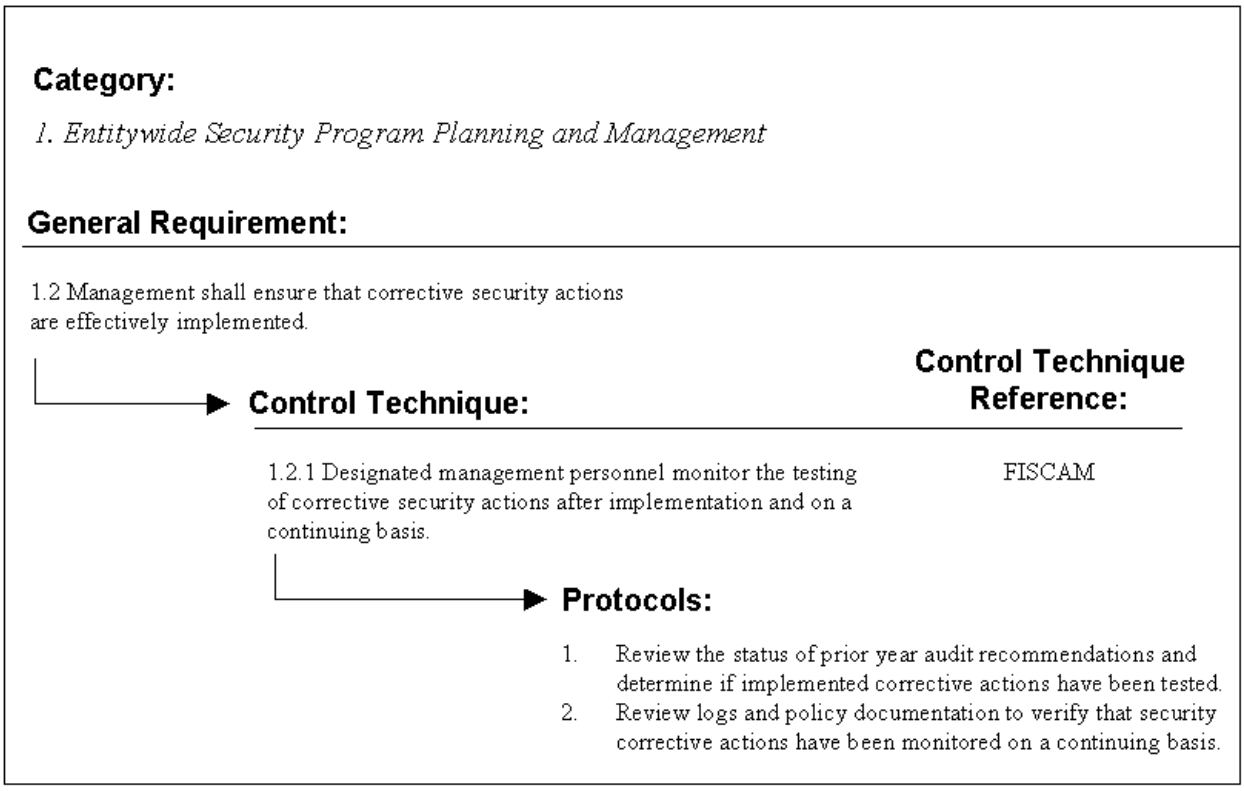

Figure A-1. Relationship Among General Requirements, Control Techniques, and Protocols

General Requirements define elements of systems or operations that must be safeguarded. The example above shows General Requirement 1.2 from the Category "Entitywide Security Program Planning and Management." The General Requirement states that, "Management shall ensure that corrective security actions are effectively implemented."

Control Techniques describe particular system elements that must be in place to consider the General Requirement valid. The example above shows Control Technique 1.2.1, which states "Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis." A business partner would be in compliance with General Requirement 1.2 if Control Technique 1.2.1 has been validated.

To assist business partners in the development of CSR responses, CMS has developed additional information to clarify common CSR issues.

- Guidance—Additional guidance has been developed to clarify issues and provide additional information regarding each CSR. This information is available in the CAST during the *self-assessment* process, and may be printed from the forms menu.
- Related CSRs—Each CSR may be related to one or more other CSRs. It may be important that CSR responses be coordinated between these related CSRs. Business partners should take care to ensure that these related CSR responses are not conflicting. This information is available in the CAST during the *self-assessment* process, and may be printed from the forms menu.
- CSR Responsibility—A matrix has been developed jointly with CMS and business partner security experts to indicate where responsibility may lie for addressing the requirement of each CSR. This matrix indicates a best estimate of whether a particular CSR is applicable to a given contract type. While this matrix is not meant to be used as a requirements document, it does give business partners and CMS reviewers an indication of whether a particular CSR should be addressed by a given business partner. This information is available in the CAST during the *self-assessment* process, and may be included in output printed from the "Print Reports."

To assist its business partners in this validation, CMS has developed Audit Protocols. Protocols are recommended *self-assessment* procedures designed to verify that sites are in compliance with system security requirements. Protocols are not security requirements; rather, they have been developed based on the same Federal and CMS security documents used to create the CMS *CSRs* and, as such, provide CMS business partners with *self-assessment* procedures that are similar to audit procedures used by CMS and external agencies.

Because CMS *CSRs* and Protocols 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, a business partner System Security Officer (SSO) could review the *CSRs* specifically associated with the IRS 1075. Additionally, by using the CAST tool (described in Section A-2 below), the SSO could use references in the CAST database to determine the location of a requirement in the IRS 1075. The SSO could also perform a preparatory *self-assessment* based only on those requirements that have the IRS 1075 as a source.

CMS continues to focus on protecting the health information received from our beneficiaries while processing claims. In FY 2005, CMS updated and added core security requirements based on CMS' Acceptable Risk Safeguards and the NISTs Security Self Assessment Guide for Information Technology Systems (NIST SP 800-26). Many of the CSR updates are not new requirements; rather, they simply restate, strengthen, or clarify current requirements.

Good practices related to ensuring the confidentiality, integrity, and availability (CIA) of information remain paramount in the continuing effort to improve the overall security program. CMS has provided technical clarifications and accounted for the potential impacts of the updated or new requirements. The following rationale was used in preparing these clarifications:

- *Where the ARS and NIST SP 800-26 were already covered by an existing CSR, these documents were added as references.*
- *Where the ARS and NIST SP 800-26 were not covered by an existing CSR, a new CSR was added and the appropriate document(s) were listed as a reference(s).*
- *Where the ARS and NIST SP 800-26 were partially covered by an existing CSR, the existing CSR was modified to incorporate inclusive language and the appropriate document(s) were listed as reference(s).*

At the current time, CMS does not anticipate any additional funding being provided to Medicare Contractors to address the new requirements. The new requirements represent best practices and we believe many contractors are already compliant or in the process of implementing changes to become compliant.

In a situation where the implementation of alternatives and/or compensating controls is not possible, the contractor's non-compliance must also be documented in the risk assessment (RA), Systems Security Plan (SSP), and the CAST self-assessment. CMS encourages Medicare contractors 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 as part of risk management and the alternative or compensating controls must be documented in the information security risk assessment, SSP, and annual CAST submissions.

See *Attachment* A for a copy of the CMS *CSRs* in Adobe Acrobat (.pdf) format.

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

CMS has made available to its business partners the CAST *self-assessment application*. *The CAST is the self-assessment module in the CMS Tool Suite which is available for download on the CMS website.* The CAST *self-assessment module* is an automated database and software application that enables business partners to perform required *self-assessment*s by entering data into electronic CAST questionnaires based on the CMS CSRs and Protocols. The business partner will provide the CAST back-end database as part of submitted certification material. The business partner will submit the CAST database to the CCMO/PO for review (along with all other required security documentation, as described in Section 3 of the CMS/Business Partners Systems Security Manual *[BPSSM]*).

The *CMS Tool Suite* provides business partners with a powerful reporting tool that generates formatted *self-assessment* forms, copies of CMS CSRs, and standardized site-analysis reports. The *CMS Tool Suite* also records information about a site, Risk Analysis and Contingency Plan reviews, and *Weakness and Action Plans* for achieving compliance with CMS CSRs.

CMS requires that business partners complete annual *self-assessment*s using CAST. These automated *self-assessment*s are performed using the CAST *self-assessment module in the CMS Tool Suite*. The CAST database includes Protocols that are designed to assist in the assessment of compliance with the CMS CSRs. The completed *self-assessment* will be included in the Security Profile (Section 3.7). Business partners can also use CAST to conduct *self-assessment*s in preparation for audits by specific external agencies. The CAST allows the business partner to generate a Q&A form that consists of those CSRs and Protocols that have a particular source document as a reference (e.g., IRS 1075, GAO FISCAM, etc.).

The *CMS Tool Suite* will be available for download from the CMS website. The Medicare *Business Partners* must complete the CAST self-assessment *module* and submit a copy on CD-ROM to the CMS Central Office and the Consortia Contractor Management Officer (CCMO) for Title XVIII contracts or the Project Officer (PO) for FAR contracts by close of business *May 27, 2005*. A copy of the CAST *self-assessment* must be placed in the System Security Profile. Please be advised that this information should not be submitted to the CMS via email. Registered mail or its equivalent should be used. Should you need technical assistance, contact the CMS/*Northrop Grumman IT* Help Desk at (703)-620-8585.

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

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

a) When entering information into *the* CAST *self-assessment*, the business partner will provide specific information in the *Response* Explanation/Comment field as to the status of compliance with the applicable requirement. CAST can then produce a pre-formatted report of *self-assessment* results and graphical analysis.

b) Each CSR requires a "Status" *(i.e., Yes, No, Partial, Planned, N/A)* to be selected, and each CSR requires a detailed explanation in the *Response* Explanation/Comment 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) Where a merging of responsibilities occurs between business partners (such as the interface between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in the *Response* Explanation/ Comments field. The description should include local responsibilities as well as those that are perceived to be responsibilities of some other CMS business partner.

d) Each CSR in the CAST includes a*n applicability matrix* that identifies the likely responsibility *for* each CSR by CMS contract type (i.e., Part A, Part B, DMERC, etc.). The purpose of the *applicability matrix* is not to summarily include or exclude CSRs from a particular contract type. The *applicability matrix* is designed only as a guide to business partners. CMS recognizes that system configurations vary widely throughout the business partner community. Therefore, each business partner must evaluate each CSR as to applicability to its own systems.

e) Business partners 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 some third-party subcontractor (such as a business services company), responsibility for the implementation of security controls ultimately resides with the primary contract holder. Business partners 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.

f) Business partners should also be aware of the CSR terms included in the BPSSM Glossary (Appendix E) and address the CSRs as they apply within 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 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 that manipulates data or performs a specific function (e.g., front-end and back-end applications).

g) 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 partners are required to enter a current status and comment or 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. In order to assist with the development of responses to the CSRs, the following decision tree has been developed to assist in the establishment of the current status of the business partner security.

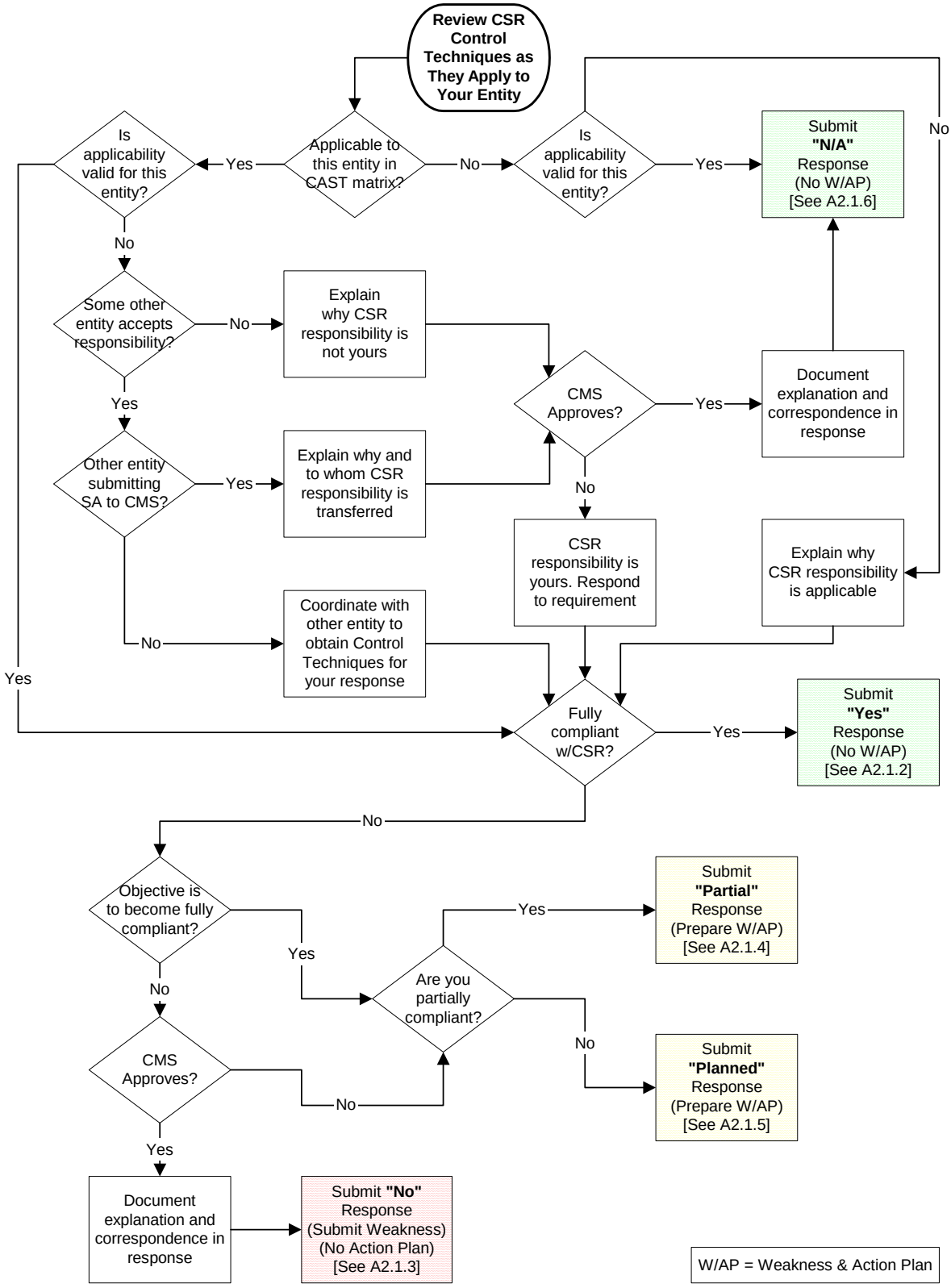

Figure A-2. "Status" Decision Tree

2.1.2 Yes Responses

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

A response status of "Yes" indicates that all of the Control Technique requirements are currently being met in their entirety with in-place measures or controls. The *Response explanation/comments* field should, at a minimum, contain a detailed explanation of the What, Where, and How. These minimum requirements are listed below:

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

Verification is central to any remedy to meet CSR compliance. Documentation in the form of logs, procedures, manuals, policies, employee training records, etc. must be available to verify compliance. A control that is not verifiable is not normally considered acceptable.

b) **Where** can 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) Explain in detail how all components of the existing controls (currently in place) are implemented to meet all aspects of the CSR as of the submittal date of the *self-assessment*. When a CSR includes multiple elements or requirements, existing controls must be explained in detail for each element or requirement in the CSR.

ii) Do not include planned controls or controls that are not fully implemented. If all components are not fully in place, the response status should be changed to "Planned" or "Partial."

iii) 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.

d) *Weakness* – The "*Weakness*" button is disabled for a response with a status of "Yes."

No additional *Weakness and Action Plan* information can or should be provided. If *there is a weakness associated with the response*, the response status should be changed to either "Partial" or "*Planned*."

Example entry for a CSR with a response status of "Yes":

"Security Awareness 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 Control Techniques as documented in company policy NG 7541-S3. The records of attendance are maintained *in cabinet #5* in the Corporate Training Office, on the fifth floor of Bldg. #5."

2.1.3 No Responses

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

A response status of "No" indicates that none of the Control Technique requirements are currently being met and there is no *Action Plan* for meeting these requirements. If the business partner does not meet the requirements of the CSR and has no plans to implement *measures* that will fully meet the CSR Control Techniques, then the response status should be "No." In this case, written notification to CMS must be provided (and acknowledged by CMS) that the CSR at issue is not currently being addressed and the business partner does not intend to meet the applicable compliance requirements. *If CMS concurs with the explanation and accepts the risk related to the "No" response status, the business partner is required to submit a Weakness for this risk but is not required to prepare an Action Plan.*

If CMS is not willing to accept the risk associated with the business partner not being in full compliance with all Control Techniques in the CSR, CMS will state so in their response and the business partner must change the CSR response status to "Partial" or "Planned," depending on if there are any existing controls (Partial) or no existing controls (Planned). In both cases, a Weakness and Action Plan must be prepared.

In all cases, the Response explanation/comments field should, at a minimum, contain a detailed explanation of the Why and How. These minimum requirements are listed below:

a) **Why** is this CSR not being fully met? What efforts are underway or have been completed in an attempt to fully resolve this issue?

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

i) CMS expects all CSRs to be addressed by all business partners. If the business partner does not meet the requirements of any CSR and has no plans to implement the CSR control techniques, written notification must be provide to CMS and acknowledged by CMS. This written notification should include a detailed explanation of why the CSR control techniques are not being met and why the business partner does not intend to implement them.

ii) Include the following information with CMS-approved "No" responses:

(1) Date CMS acknowledged the response,

(2) CMS office that acknowledged the response, and

(3) Method of CMS acknowledgement (e.g., e-mail, letter, phone call).

iii) Describe any circumstances that may have prevented implementation of a suitable control to date. While this explanation will not alleviate responsibility for the CSR, it will reduce inquiries by CMS during the evaluation phase of business partner *self-assessments*.

c) *Weakness* – The "*Weakness*" button is enabled for a response with a status of "No." *A Weakness must* be developed to address the CSR.

Example entry for a CSR with a response status of "No":

"Our file server system uses a Green Hat Linux 1.0 operating system. This version of Linux is hard-coded to display the password while entering. G. Iam Secure [(401)

555-1234] contacted (via phone) I. M. Programmer at Green Hat [(651) 555-4321] on 8/31/00 to determine if an update to correct this discrepancy is underway. Mr. Programmer indicated that the password will continue to be displayed through the next revision, but future changes are tentatively planned. Investigation into alternative software has resulted in no suitable software packages. CMS was informed in writing on 9/30/00 and CMS acknowledged in writing *and accepted the risk associated with this weakness* on 10/15/00. Applicable correspondences are maintained in file cabinet 8b on the third floor of the Operations Building."

2.1.4 Partial Responses

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

A response status of "Partial" indicates that not all of the Control Technique requirements are currently being met in their entirety, but efforts are either already underway to meet full compliance or additional controls are required. This can simply mean that one or more portions of a CSR are not being met, or it may mean that the requirements are being addressed and controls are implemented, but not throughout the entire enterprise. If the business partner does not plan to fully comply with this CSR, this CSR response status should be changed to "No." Be clear and complete with these comments as this explanation will be part of the *Weakness and Action Plan* as well as the *self-assessment* submitted to CMS. The *Response* Explanation/ Comments field should, at a minimum, contain a detailed explanation of the What, Where, Why, and How. These minimum requirements are listed below:

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

Verification is central to any remedy to meet CSR compliance. Documentation in the form of logs, procedures, manuals, policies, employee training records, etc. must be available to verify compliance. A control that is not verifiable is not normally considered acceptable.

b) **Where** can 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) **Why** is this CSR not being fully met? What efforts are underway or have been completed in an attempt to fully resolve this issue?

d) **How** exactly is the CSR partially met?

i) Explain in detail how all components of existing controls (currently in place) are implemented to meet those aspects of the CSR that are fully implemented as of the submittal date of the *self-assessment*. When a CSR includes multiple elements or requirements, existing controls must be explained in detail for each element or requirement in the CSR.

ii) Describe in detail how the remaining Control Techniques will be brought into compliance.

iii) 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.

f) *Weakness* – The "*Weakness*" button is enabled for a response with a status of "Partial." *A Weakness and Action Plan must be developed to address the CSR.*

Example entry for a CSR with a response status of "Partial":

"We use a mainframe and an off-site data storage facility connected via a T1 line and triple-DES encryption. The local corporate distributed network (WAN), which may process some administrative documents containing sensitive patient information, is connected via DSL and T1 lines to remote facilities without encryption. *Triple*-DES

encryption devices *have been purchased* for the mainframe system as well as for network encryption devices for the local corporate distributed LAN. The mainframe encryption devices were installed on 11/14/02 but the LAN network encryption devices are currently on back order. Documentation on our existing and planned encryption techniques is maintained *in cabinet #2* in the Security Department, on the second floor of Bldg. #2."

2.1.5 Planned Responses

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

A response status of "Planned" indicates that while none of the Control Technique requirements are currently being met *but* a*n Action Plan* exists to remedy the situation. The *Response* Explanation/ Comments field should, at a minimum, contain a detailed explanation of the What, Where, Why, and How. These minimum requirements are listed below:

a) **What** can be used to verify the planned compliance?

Verification is central to any remedy to meet CSR compliance. Documentation in the form of a funded plan must be available to verify planned compliance. A control that is not verifiable is not normally considered acceptable.

b) **Where** can the *Action Plan* be found?

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

c) **Why** is this CSR not being met? What efforts are underway in an attempt to fully resolve this issue? *Describe any circumstances that may have prevented implementation of a suitable control to date. While this explanation will not alleviate responsibility for the CSR, it will reduce inquiries by CMS during the evaluation phase of business partner* self-assessments.

d) **How** exactly will this CSR be met?

i) Explain in detail how all components of the planned controls will be implemented. When a CSR includes multiple elements or requirements, planned controls must be explained in detail for each element or requirement in the CSR.

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.

f) *Weakness* – The "*Weakness*" button is *enabled* for a response with a status of "Planned." *A Weakness and Action Plan must be developed to address the CSR.*

Example entry for a CSR with a response status of "Planned":

"A training plan and training materials do not exist for new employee orientation training. New employee training is being developed in a joint effort between the Security Department and the IT Training Department. The security training outline is complete and on file *in cabinet #5* in the Corporate Training Office on the fifth floor of Bldg. #5. No additional funding is required to meet the requirements of this CSR."

2.1.6 N/A Responses

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

A response status of "N/A" indicates that the Control Technique requirements are not applicable to this *entity*. Except as indicated in the CAST CSR *Applicability* matrix, *CMS expects* most, if not all, CSRs *to* apply to all portions of all business partner contracts. *Very few CSRs are expected to receive occasional "N/A" responses based on answers provided in alternative CSRs (see example).* Where an intersection of responsibilities occurs between business partners (such as the interface between Data Centers and claims processors or between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in the *Response explanation/comments* field *(as it applies to this contract type)*. When Control Technique requirements have been subcontracted out to a third-party contractor or are being performed for this contract entity by another corporate entity, the ultimate responsibility for implementing and reporting compliance (or non-compliance) remains with the primary contract holder, so the response must be some status other than "N/A." The *Response explanation/comments* field should contain a detailed explanation of the Why and How. These requirements are listed 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 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 applicability matrix.*

Where a merging of responsibilities occurs between business partners (such as the interface between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in the Response explanation/comments field (as it applies to this contract type). Note that even if data processing duties are subcontracted out to either another CMS business partner (such as a Data Center) or to some third-party subcontractor (such as a business services company), responsibility for the implementation of security controls ultimately resides with the primary contract holder.

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

i. CMS approvals (and the citation[s] thereof) are not required for N/A responses that are corroborated by the applicability matrix.

ii. 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 cited (see below). Note that CMS approval must be re-obtained each year for each CSR whose applicability is to be waived for the business partner. Approvals for prior years may not be cited.

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) Method of CMS approval (e.g., e-mail, letter, phone call).

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" (CSR 2.2.19 and 2.2.5). This issue was discussed via letter to CMS (12/15/98) and agreed to by the Regional Office (2/4/99). Both letters are on file *in cabinet #3* in the Security Office located on the third floor of Bldg. #3."

2.2 Weakness

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

All compliance issues will result in a weakness and corresponding Action Plans. These will be addressed in the Tool Suite User Guide and the training made available to the CMS Business partners. Further clarification is available in the main section of the BPSSM.

Appendix B:
Medicare Information Technology (IT) Systems Contingency Planning

Table of Contents

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

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 complet*ing* the IT systems contingency planning process.

5.0 Medicare IT Systems Contingency Plan

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

The following format m*ay* 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 address the fact that off-site storage must be provided for:

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

6.1 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.

6.5 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
- e
- 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 *a*ction *management process*
- Retest plans
- Memos of Understanding/Formal Test Arrangements.

8.1 Business Partner Management

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

- 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 contingency plan
    - Changes to the contingency plan
    - Test Plans
    - Test *r*esults
    - Corrective *a*ction *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. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

- 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
- Assures that the plan is updated based on test results.

12.0 References

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

*In addition to this manual, t*he 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.
- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, Section 3.6.

  http://www.gao.gov/special.pubs/ail12_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
- 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 E:
Glossary

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

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 (IS) resource. (NSTISSI)
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)
2.3 *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.

Term	Definition
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)
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.

Term	Definition
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. (NSTISSI)
2.4 *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.

Term	Definition
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.
2.5 *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: 1. Operation of user code in master mode. 2. Unauthorized acquisition of identification password or file access passwords. 3. Accessing a file without using prescribed operating system mechanisms. 4. 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. CMS business partners are Shared Systems Maintainers (SSM), CWF host sites, DMERC, Data Centers and other specialty contractors.

Term	Definition
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.
2.6 *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. (NSTISSI)
Code	Instructions written in a computer programming language. (See object code and source code.) (FISCAM)
Cold Site	An IS 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)
2.7 *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 persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (NSTISSI)
Compact Disc-Read Only Memory (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally read-only. (FISCAM)

Term	Definition
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 are 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.

Term	Definition
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 are 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)
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.

Term	Definition
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)

Term	Definition
Data Control	The function responsible for seeing that all data necessary for processing is 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 its meaning, 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.
2.8 *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)

Term	Definition
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.

Term	Definition
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)
2.9 *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.
2.10 *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)

Term	Definition
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.

Term	Definition
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)

Term	Definition
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 information technology, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. (FISCAM)
2.11 *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.

Term	Definition
Information Systems (IS)	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (NSTISSI)
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) (Also see Systems Security)
Information Systems Security Officer (ISSO)	(1) Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer. (NSTISSI)
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, its 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)

Term	Definition
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. (NSTISSI)
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)

Term	Definition
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)

Term	Definition
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 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)

Term	Definition
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)

Term	Definition
2.12 *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 is stored or transported. The risk to exposure is considered greater when data is in an electronically readable and transmittable form than when the same data is 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)

Term	Definition
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. (NSTISSI)
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.

Term	Definition
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)
2.13 *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)
2.14 *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. (NSTISSI)

Term	Definition
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.
2.15 *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)

Term	Definition
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 IS or its users. (NSTISSI)
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	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)
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)

Term	Definition
Project Officer	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 Regional Carriers (DMERCs), 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. (NSTISSI)
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)

Term	Definition
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 IS and computational capability after a system failure. (NSTISSI)
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)

Term	Definition
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)

Term	Definition
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.

Term	Definition
SDLC methodology	See System Development Life Cycle Methodology.
Security	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)
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)

Term	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	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)
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (NSTISSI)
Security Requirements Baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security. (NSTISSI)
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 information technology 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)

Term	Definition
Sensitive Data	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)
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 of Data	The need to protect data from unauthorized disclosure, fraud, waste, or abuse.
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)

Term	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 =** 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)

Term	Definition
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.

Term	Definition
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.

Term	Definition
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 an 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.
System 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.
Systems 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) (Also see IS Security Plan and System Security Plan)
System Security Profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS. (NSTISSI)
Tape Library	The physical site where magnetic media is stored. (FISCAM)
2.16 *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)

Term	Definition
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)
2.17 *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. (NSTISSI)
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)

Term	Definition
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. (NSTISSI)
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)
2.18 *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)

Term	Definition
Vulnerability	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)
WAN	See Wide Area Network.
Warning Banner	NIST Special Publication 800-12 Footnote 131: The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. The ambiguity results from the fact that current laws were written years before such concerns as keystroke monitoring or system intruders became prevalent. Additionally, no legal precedent has been set to determine whether keystroke monitoring is legal or illegal. System administrators conducting such monitoring might be subject to criminal and civil liabilities. The Department of Justice advises system administrators to protect themselves by giving notice to system users if keystroke monitoring is being conducted. Notice should include agency/organization policy statements, training on the subject, and a **banner** notice on each system being monitored. [NIST, CSL Bulletin, March 1993]
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)

Term	Definition
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 IS that results only in the flow of information from a subject to an object. (NSTISSI)
Write Access	Permission to write to an object in an IS. (NSTISSI)

References:

1. NCSC-TG-004 **–** Rainbow Series, Aqua Book, **Glossary of Computer Security Terms,** NCSC-TG-004-88, Library No. S-231, 238**.** Issued by the National Computer Security Center (NCSC).
2. FISCAM – Federal Information System Controls Audit Manual, GAO/AIMD-12.19.6
3. AISSP – Automated Information Systems Security Program Handbook, DHHS, *http://wwwoirm.nih.gov/policy/aissp.html*, (for Source references see document)
4. Micki Krause and Harold F. Tipton, Handbook of Information Security Management (HISM), Imprint: Auerbach Publications, Publisher: CRC Press LLC, ISBN: 0849399475.
5. DoN - Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A, Aug. 3,1982. (Glossary)
6. NSTISSI – National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999 (Revision 1)
7. TechEncy – Technical Encyclopedia of definitions supported by TechWeb.com
8. GLOSSARY - The definitions in this glossary are drawn from several sources, including this manual, certain IBM manuals, and the documents and sources listed in the bibliography. In addition, certain definitions were developed by project staff and independent public accounting firms.

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference

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).	1. Review training syllabus for inclusion of the required training. 2. Review a sample of training records to confirm completion of the required training. 3. Review documented procedure for generation of security reminders. 4. Review the training policy. 5. Interview a sample of site personnel to verify that documented training was received.	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) FISCAM TSP-4.2.2 PDD 63 358 ARS 4.1 ARS 4.3 NIST 800-26 13.1.4

Guidance: A formal program should be established with a policy and a procedure. Related CSRs: 5.12.1, 2.9.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.1.2	Security skill needs are accurately identified and included in job descriptions.	1. Review a sample of job descriptions for identification of security skills required. 2. Evaluate the apparent relevance of the specified security skills to the job described.	FISCAM TSP-4.2.1

Guidance: The SSO should work in conjunction with the HR department on job description updates. Related CSRs: 3.3.3, 3.6.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.1.3	All personnel (employees and contractors) are provided security awareness and security training prior to being allowed access to CMS sensitive information or data, and security awareness is repeated, minimally, on an annual basis.	1. Review training syllabus for inclusion of security awareness training. 2. Review policies and procedures for inclusion of the required process. 3. For a sample of personnel having access to sensitive information, review personnel records for documentation of receipt of security awareness training. 4. For a sample of personnel having access to sensitive information, review training documentation and job descriptions for apparent customization of security awareness training to job responsibilities. 5. Interview a sample of personnel having access to sensitive information to determine if they are aware of their responsibilities relating to handling of sensitive information. 6. Verify that records show training occurred prior to access to sensitive data.	FISCAM TSP-3.3.1 IRS 1075 6.2@1 CMS Directed PDD 63 358 HIPAA 164.308(a)(5)(i) ARS 4.4 NIST 800-26 13.1.3

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.1.4 Security training 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).	For a sample of personnel, review training documentation and job descriptions for evidence of customization of security training to the level of job responsibilities.	CMS Directed NIST 800-26 13.1
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).		Related CSRs: 3.2.1, 3.2.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.5 The employees acknowledge, in writing, having received the security and awareness training.	1. Verify that records show all employees have acknowledged receiving security and awareness training. 2. Check a random sample of employees records to verify training attendance signature.	FISCAM TSP-4.2.3 CMS Directed ARS 4.1 ARS 4.3 NIST 800-26 13.1.2
Guidance: No further guidance required.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.6 A record of the security awareness and security training subject(s) covered is maintained.	Verify that records are being maintained that document the security awareness and security training subjects covered.	CMS Directed
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.7 Training in emergency procedures is conducted at least once a year.	Verify the emergency procedures are dealt with in the COOP.	CMS Directed NIST 800-26 12.1.8
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.		Related CSRs: 5.6.1, 5.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.8 Policy and security training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided.	Review documentation of policy and training to confirm the protection of copyright information under the terms of the provision of the copyright holder.	CMS Directed
Guidance: A security policy should exist, and security training should include, appropriate information regarding copyright protection.		Related CSRs: 3.3.1, 7.1.2, 10.7.2, 2.2.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.9 When individuals are authorized to bypass significant technical and operational controls, or when controls cannot adequately protect the information, the affected individuals are screened prior to access and periodically thereafter.	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.	NIST 800-26 6.2.1 NIST 800-26 6.2.3
Guidance: Screening should be consistent with the criteria established for the sensitivity designation of the assigned position.		Related CSRs: 1.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.10 A help desk or user support group is available to offer advice.	Interview a sampling of users to determine if a help desk or support group is available to offer advice.	NIST 800-26 8.1 NIST 800-26 8.1.1
Guidance: Possible implementations of incident support resources include a help desk or support group.		Related CSRs: 2.9.18
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference
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.	1. Records providing information on the monitoring activities should be available. 2. Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested. 3. Review logs and policy documentation to verify that security corrective actions have been monitored on a continuing basis.	FISCAM TSP-5.2 HIPAA 164.316(b)(2)(iii)
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.	Related CSRs: 1.8.7, 1.12.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.2.2 There is an effective and timely process for reporting significant weaknesses and ensuring effective remedial action.	1. Review audit and review findings for their inclusion in the POA&M. 2. Review relevant policies and procedures for inclusion of the required process.	NIST 800-26 2.2.1
Guidance: The Plan of Action and Milestones (POA&M) updates are based on the findings from security control assessments, security impact analysis, and continuous monitoring activities.	Related CSRs: 2.1.1, 2.13.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.2.3 Budget requests (e.g., Line One funding, safeguards) include the security resources required for the system.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review budget requests for inclusion of security resources necessary for the system.	NIST 800-26 3.1.5
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.	Related CSRs: 4.6.2	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.2.4 Security controls are consistent with, and an integral part of, the IT architecture of the business partner.	Review relevant policies and procedures for inclusion of the required process.	NIST 800-26 3.1.9
Guidance: The information system-required documentation includes security configuration settings and security implementation guidance. They should also provide the required security capabilities and required design and development processes.	Related CSRs: 6.3.4	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement Control Technique	Protocol	Reference
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.)	1. Review disclosure list for entries indicating that the documented process has been followed. 2. Interview responsible individual(s) to confirm understanding of the required procedure. 3. Review relevant policies and procedures for inclusion of the required logging process elements. 4. For a sample of documents being received from the IRS, observe handling of receipt of sensitive information for compliance with established procedures.	IRS 1075 3.3@2.2
Guidance: Transmission of Federal Tax Information must be accompanied by appropriate records that will determine who released the information and what was released.	Related CSRs:	
☐ ***SS*** ☐ ***PSC*** ☐ ***PartB*** ☐ ***PartA*** ☐ ***Dmerc*** ☐ ***DC*** ☐ ***CWF*** ☑ ***COB***		
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.	1. Observe transmittal of sensitive information for compliance with established procedures. 2. Review relevant policies and procedures for inclusion of the required logging process elements. 3. Review disclosure list for entries indicating that the documented process has been followed. 4. Interview responsible individual(s) to confirm understanding of the required procedure.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(I) IRS 1075 3.3@2.1 HIPAA 164.312(c)(1) ARS 11.6
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.	Related CSRs: 2.12.2	
☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
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 for the logging of shipping and receipts and a periodic reconciliation of these records.	1. Evaluate the identified control procedures for inclusions of maintenance of records logging all shipping and receipts, and of periodic reconciliation of these records. 2. Review documented procedures for control of sensitive data entering or leaving the facility. 3. Evaluate the identified control procedures for inclusions of specific protections against erroneous or unauthorized transfers. 4. Review policy for relevance.	CMS Directed HIPAA 164.310(d)(2)(iii) NIST 800-26 8.2.2
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.	Related CSRs: 2.2.25, 2.2.26	
☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.3.4 A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.	1. Review the documented procedure for destruction of data. 2. Verify that the reviewed procedure includes protections against sensitive data becoming available to unauthorized personnel.	CMS Directed ARS 1.6
Guidance: A good concept is to establish a formal program with a policy and procedures for developing and maintaining records. A record should be maintained that verifies who performed the destruction and when sensitive information was destroyed.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.3.5 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. Ensure the destruction of any sensitive information hard copy documents when no longer needed.	1. Review disposal procedures for inclusion of use of approved destruction methods during disposal of hard copy documents that are no longer needed. 2. For a sample of employees, interview to determine that disposal procedures are known and being followed. 3. Review disposal procedures for inclusion of use of approved sanitization procedures before release of any nonvolatile storage devices or media. 4. Review disposal procedures for inclusion of protections against use of retired, discarded, or unneeded sensitive data by unauthorized persons.	HIPAA 164.312(c)(2) IRS 1075 6.3@6 HIPAA 164.312(e)(2)(i) CMS Directed HIPAA 164.310(d)(2)(i) HIPAA 164.310(d)(2)(ii) HIPAA 164.312(c)(1) ARS 9.6 NIST 800-26 3.2.11 NIST 800-26 8.2.8 NIST 800-26 10.1.3
Guidance: A good approach assures policies and procedures exist for release and/or destruction of CMS sensitive information.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.3.6 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]).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. By inspection confirm that the specified data and records are stored on-site.	CMS Directed
Guidance: When utilizing commercial storage facilities for off-site storage, ensure that any agreements in place address these Federal standards.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.3.7 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review a sample of destruction records to confirm consistent use of the procedure.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.308(a)(4)(i) HIPAA 164.310(d)(2)(ii) HIPAA 164.310(d)(2)(iii) IRS 1075 8.4@1 HIPAA 164.312(c)(1) ARS 9.5
Guidance: A formal program should be established with a policy and procedure. Review and update existing policy and procedures for addressing these requirements.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference
1.3.8 Before releasing files containing sensitive information to an individual or contractor not authorized to access sensitive information, care is taken to remove all such sensitive information. 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 log is used to document that all discarded or transferred items are examined for sensitive information and this information is cleared before the items are released.	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.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(d)(2)(i) HIPAA 164.310(d)(2)(ii) IRS 1075 5.3@2.3 FISCAM TAC-3.4 HIPAA 164.312(c)(1) ARS 1.6 ARS 9.5 NIST 800-26 3.2.12 NIST 800-26 3.2.13 NIST 800-26 8.2.9

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.

Related CSRs: 2.12.2, 2.14.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.9 FTI is physically destroyed by authorized personnel, or returned to the originator or to the system security administrator. (This CSR applies only to the COB contractor.)	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.	IRS 1075 6.3@6

Guidance: A formal security program should be established with a policy and procedure.

Related CSRs:

☐ *SS* ☐ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

1.3.10 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. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)	1. Confirm by inspection that facility has latest version of IRS Publication 1075. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming consistent use of the required receipt process.	IRS 1075 8.1

Guidance: It is a good approach when returning FTI information to CMS 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.

Related CSRs:

☐ *SS* ☐ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

1.3.11 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.	1. Review documentation confirming that destruction is accomplished using one or more of the approved methods. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) IRS 1075 8.3 HIPAA 164.312(c)(1) ARS 9.6 NIST 800-26 8.2.10

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
1.3.12 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 recorded in a log 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 log 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 logged.	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.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(d)(2)(iii) IRS 1075 4.6@3 HIPAA 164.312(c)(1) FISCAM TAC-3.1.A.6 CMS Directed IRS 1075 3.2@1.3 IRS 1075 3.2@2.2 PDD 63 193 ARS 1.6 NIST 800-26 8.2 NIST 800-26 8.2.7 NIST 800-26 10.2.9

Guidance: One method would be to ensure that deposits and withdrawals of tapes and other storage media from the library are authorized and logged and that audit trails kept as part of inventory management.

Related CSRs: 1.5.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.13 Semiannual inventories of removable storage devices and media containing sensitive information are performed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.	IRS 1075 3.2@2.3 PDD 63 193

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.14 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.	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.	IRS 1075 3.2@1.1 PDD 63 193

Guidance: A formal program should be established with a policy and procedure.

Related CSRs: 2.2.31

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.15 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. Media holding, processing or storing sensitive data is kept in a secure area.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming location of computer operations are in a secure area with restricted access, or that establishes approved use of equivalent safeguards.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(a)(1) HIPAA 164.310(c) IRS 1075 4.6@1.2 IRS 1075 4.6@1.5 HIPAA 164.312(c)(1) PDD 63 193 CMS Directed ARS 9.3 ARS 9.4 ARS 9.7 NIST 800-26 8.2 NIST 800-26 8.2.7 NIST 800-26 10.2.9

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).

Related CSRs: 2.2.16, 2.5.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
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.	1. Review a sample of training records to confirm completion of security awareness training. 2. Review training syllabus for inclusion of the security awareness training. 3. Review relevant policies and procedures for inclusion of the prescribed features. 4. Review personnel security records and job descriptions to verify that operating and maintenance personnel have the proper clearances. 5. Review access and maintenance logs, and interview a sample of operating and maintenance personnel, to verify that all maintenance access is logged, and that all maintenance is performed or supervised by authorized, knowledgeable personnel. 6. Review the process for requesting, establishing, issuing, and closing user accounts.	HIPAA 164.308(a)(3)(i) HIPAA 164.308(a)(3)(ii)(A) HIPAA 164.308(a)(3)(ii)(B) ARS 1.5 ARS 1.6 ARS 1.7 ARS 3.13 ARS 4.1 ARS 4.3 NIST 800-26 6.1.8 NIST 800-26 10.1 NIST 800-26 10.1.1 NIST 800-26 10.1.3
Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information.		Related CSRs: 4.2.2, 1.8.4, 2.2.19, 3.5.2, 5.9.9, 2.8.3, 2.8.5, 2.8.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.2 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.	1. Review relevant policies and procedures for inclusion of the required self assessment process. 2. Review documentation confirming submittal of the most recent self assessment to CMS.	HIPAA 164.316(b)(2)(iii) IRS 1075 6.3@1 HIPAA 164.308(a)(8) NIST 800-26 2.1.3
Guidance: Annually complete the self assessment utilizing the Contractor Assessment Security Tool (CAST), and run the "Error Check Self-Assessments."		Related CSRs: 2.12.1, 1.8.6, 2.5.7, 2.5.8, 2.5.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.3 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.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm familiarity with the policy and how to report such improper activity.	IRS 1075 10.1 HIPAA 164.308(a)(6)(ii) FISCAM TAC-4.3.3
Guidance: Establish procedures to identify apparent security violations and ensure that suspicious activity is investigated and appropriate action taken.		Related CSRs: 1.4.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.4 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.	1. Review policies and procedures for the required distribution process(es). 2. Review the distributed security policies for inclusion of the required rules. 3. Interview a sample of site personnel to verify that security policies are distributed.	FISCAM TSP-3.3.2 HIPAA 164.308(a)(1)(i) NIST 800-26 4.1.3 NIST 800-26 13.1.1 NIST 800-26 13.1.5
Guidance: Establish procedures to distribute the security policies to all necessary personnel, and develop a process to document the receipt by the personnel.		Related CSRs: 6.4.1, 6.3.9, 9.6.1, 1.5.1, 1.9.11
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference
1.4.5 Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. 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.	Review relevant policies and procedures for inclusion and directed use of the required procedures.	CMS Directed HIPAA 164.308(a)(6)(i) HIPAA 164.308(a)(6)(ii) ARS 10.5

Guidance: A good approach is to access the CERT WEB site for sample procedures for inclusion. Related CSRs: 1.6.3, 1.4.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.4.6 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.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm awareness of, and adherence to this policy.	CMS Directed

Guidance: Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business. Related CSRs: 2.9.13

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.4.7 Employees are made aware that company policy prohibits the browsing of sensitive data files for any reason other than Medicare business.	1. Interview a sample of employees to confirm awareness of, and adherence to this policy. 2. Review relevant policies for inclusion of the required directive.	CMS Directed

Guidance: Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business. The employee should have a valid need-to-know. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 responsibilities and expected behaviors 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.	1. 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. 2. 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.	FISCAM TSP-3.2 ARS 3.1

Guidance: Ensure that the Rules of Behavior are contained in the SSP and that they clearly define the responsibility of all employees. Related CSRs: 1.4.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	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.	FISCAM TSP-3.1.2 CMS Directed HIPAA 164.308(a)(2) ARS 4.6 NIST 800-26 4.1.6

Guidance: An approach is to certify or ascertain that the SSO has a CISA, CISSP or other appropriate information security certification. Related CSRs: 9.6.3, 9.6.5, 9.6.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.5.3 If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.	1. If these additional SSO positions exist, review documentation supporting use of the specified process. 2. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed ARS 4.6
Guidance: Ensure that all Medicare related actions are cleared through the primary Medicare SSO. Related CSRs:		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.4 The SSO is organizationally independent of IS operations.	Review documentation supporting the required organizational independence.	CMS Directed
Guidance: Ensure that the SSO's duties allow him/her to act independent of IS operations. Related CSRs: 1.9.10		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.5 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.	1. Review documentation supporting SSO performance of each of the specified roles and responsibilities. 2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.	HIPAA 164.316(b)(2)(iii) CMS Directed
Guidance: An approach is to include these in the SSO's job description. Related CSRs: 9.6.3, 3.1.2, 1.9.4		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.6 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.	1. Review relevant documentation for designation of this security officer. 2. Review relevant policies and procedures for inclusion of identification of the specified roles and responsibilities of this security officer.	CMS Directed ARS 10.8
Guidance: An approach is to include these in the SSO's job description. Related CSRs: 6.3.13		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.7 Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.	Review documentation supporting designation of this responsibility to specific employees.	IRS 1075 3.2@1.2 FISCAM TAC-3.1.A.3 HIPAA 164.308(a)(2) HIPAA 164.310(d)(1)
Guidance: A good approach is to have the SSO designate specific employees this responsibility. Related CSRs: 1.3.12, 2.2.31		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.5.8 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.	1. Review documentation supporting SSO performance of each of the specified roles and responsibilities. 2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities. 3. Review contracts, RFPs, and other solicitation documentation for inclusion of the specified requirements.	ARS 3.3 NIST 800-26 3.1.10 NIST 800-26 3.1.11 NIST 800-26 3.1.12 HIPAA 164.308(b)(1) HIPAA 164.308(b)(4) HIPAA 164.314(a)(1)
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.		Related CSRs: 1.11.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

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.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Review security incident procedures	HIPAA 164.308(a)(1)(ii)(D) HIPAA 164.308(a)(6)(i) ARS 4.8 ARS 10.5 NIST 800-26 14.1.6
Guidance: Refer to sample procedures from the CERT website.		Related CSRs: 1.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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 means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; (5) links to other relevant groups; and (6) receipt and response to other pertinent security alerts/advisories.	Review documentation supporting existence of the required characteristics within the Business Partner's incident response capability.	FISCAM TSP-3.4 ARS 1.9 ARS 4.8 ARS 10.5 NIST 800-26 2.1.5 NIST 800-26 14.1 NIST 800-26 14.1.1 NIST 800-26 14.1.2 NIST 800-26 14.1.3 NIST 800-26 14.1.4 NIST 800-26 14.1.5
Guidance: Refer to sample procedures from the CERT WEB site.		Related CSRs: 1.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.6.3 Relevant security incident information is documented according to 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.	1. Review Incident Handling procedures. 2. Interview response team personnel. 3. Examine secure storage area.	ARS 10.6
Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.		Related CSRs: 1.6.2, 1.4.5, 1.6.1, 1.9.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

1.7 Sensitive data to be protected shall be divided into Security levels as appropriate.

1.7.1 CMS has categorized sensitive Medicare data, FTI, and Privacy Act-protected data as sensitive information. These items are to be protected under the CMS Level 3 - High Sensitive security designation.	Sensitive Information Safeguard Requirements verify that the combinations of protection implemented for Level 3 sensitive data match those specified in the Business Partners Systems Security Manual, Section 4.1.1.3.	FISCAM TAC-1.1 IRS 1075 4.1@2 CMS Directed
Guidance: Ensure that a policy and procedure exist to categorize and protect all Medicare sensitive data as level 3 (See BPSSM).		Related CSRs: 2.5.2, 2.7.1, 2.2.7, 10.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference

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.	Review relevant policies and procedures for inclusion of the required security management features.	HIPAA 164.308(a)(1)(ii)(A) HIPAA 164.308(a)(1)(ii)(B) HIPAA 164.308(a)(1)(ii)(C) ARS 3.1 ARS 3.6

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Related CSRs: 3.1.2, 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.2	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.)	Confirm by inspection that the required documentation and agreements is on file.	FISCAM TSP-1.3 HIPAA 164.308(a)(1)(ii)(A) NIST 800-26 1.2.1 NIST 800-26 3.1.8

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Related CSRs: 3.1.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.3	The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	1. Review risk assessment policy for inclusion of the required factors. 2. Review the most recent high-level risk assessment for documentation of consideration of the required factors.	FISCAM TSP-1.2 HIPAA 164.308(a)(1)(ii)(A) ARS 3.2 NIST 800-26 1.1.3 NIST 800-26 4.1.7

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Related CSRs: 3.1.2, 2.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.4	A 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 trails/logs, 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).	1. Review relevant policies and procedures for inclusion and directed use of the required process for determining the need for reassessment. 2. Review relevant policies and procedures for inclusion and directed use of the required content. 3. Review the most recent risk assessment for documented inclusion of the required content.	CMS Directed FISCAM TSP-5.1.1 HIPAA 164.308(a)(1)(ii)(A) FISCAM TSP-1.1 PDD 63 165 ARS 5.3 ARS 9.5 ARS 10.8 NIST 800-26 1.1.2 NIST 800-26 3.1.7 NIST 800-26 4.1.1 NIST 800-26 4.1.2

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Related CSRs: 3.1.2, 3.1.3, 1.4.1, 2.2.19, 3.5.2, 5.9.9, 1.12.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.5	Facilities housing sensitive and critical resources have been identified. 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. Adequate physical security controls have been implemented that are commensurate with the risks of physical damage or access.	1. Review documentation supporting an assessment that all facilities housing sensitive and critical resources have been identified. 2. 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.	FISCAM TAC-3.1.A.1 FISCAM TAC-3.1.A.2 ARS 1.1 ARS 1.3 NIST 800-26 1.1.4 NIST 800-26 7.1

Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.

Related CSRs: 1.9.3, 1.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.8.6 A compliance review and self-assessment is conducted once a year.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming execution of the review process at least once a year.	CMS Directed

Guidance: Ensure that the CAST is completed once a year and that it is independently verified. Related CSRs: 1.4.2, 2.5.7, 2.5.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.7 Top management initiates prompt actions to correct deficiencies and ensures that corrective actions are effectively implemented.	1. Review documentation supporting consistent prompt action by top management to correct deficiencies. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSP-5.1.4 NIST 800-26 2.2 NIST 800-26 4.2.1

Guidance: An approach is to have senior management approve the corrective action plan and have quarterly updates to the plan. Related CSRs: 1.2.1, 1.12.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.8 Major systems and applications are approved by the managers whose missions they support.	1. Inspect documentation of approval for each major system and application by the specified manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSP-5.1.3

Guidance: Refer to the CMS SSPM for additional information guidance. Related CSRs: 1.9.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.9 Local Information System risk factors are periodically assessed in accordance with the CMS Information Security Risk Assessment (RA) Methodology and NIST SP 800-30.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying assessment of local risk factors in accordance with the reference.	CMS Directed ARS 5.2 NIST 800-26 1.1 NIST 800-26 12.2.4

Guidance: This CSR should be addressed as part of a formal Risk Management Program. Related CSRs: 1.9.8, 1.9.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.10 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 CMS Level 3 - High Sensitivity security designation.	Review documentation establishing that a location-specific Risk Analysis was conducted in development of each applicable System Security Plan.	CMS Directed IRS 1075 4.2 ARS 3.2

Guidance: See the Business Partners Security Manual for additional information and guidance. Related CSRs: 2.2.11, 2.2.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.1 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.	1. Review the security plan for inclusion of the required elements. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation supporting completion of the required security testing. 4. Review system configuration documentation for inclusion of links to other systems.	HIPAA 164.308(a)(5)(ii)(B) HIPAA 164.310(a)(2)(iv) ARS 3.4 ARS 3.13 NIST 800-26 1.1.1

Guidance: Policies and Procedures should exist that address these control objectives. Related CSRs: 5.9.3, 5.12.1, 2.5.1, 6.3.14

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.9.2 Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.	Review relevant policies and procedures for inclusion and directed use of the required process.	HIPAA 164.308(a)(1)(ii)(A) ARS 3.13
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.11.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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) personnel controls/personnel security; (d) incident response capability; (e) continuity of support/contingency planning; (f) technical security/technical controls; (g) system interconnection/information sharing; (h) public access controls.	1. Review documentation verifying that a security plan covers all major facilities and operations. 2. Review documentation verifying that the security plan has been approved by all key affected parties. 3. Inspect the security plan to confirm that it covers all of the specified topics.	FISCAM TSP-2.1 HIPAA 164.310(a)(1) HIPAA 164.310(a)(2(ii) HIPAA 164.310(a)(2(i) HIPAA 164.308(a)(4)(i) ARS 3.13 ARS 4.7 ARS 4.8
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.8.8, 6.1.2, 6.3.4, 10.7.3, 2.10.6, 1.6.3, 1.8.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.4 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).	1. Review documentation establishing that preparation of the plan was in accordance with the CMS SSP Methodology. 2. Review documentation verifying coverage by system security plans for all applications categorized as MA and GSS. 3. Review SSP to determine if approval signatures are included	CMS Directed ARS 1.9 ARS 3.13 ARS 5.6 NIST 800-26 3.2.8 NIST 800-26 4.1.5 NIST 800-26 5.1 NIST 800-26 5.1.2 NIST 800-26 12.2.1
Guidance: Refer to the CMS System Security Plans Methodology for further guidance.		Related CSRs: 9.4.1, 3.2.4, 3.3.2, 3.4.6, 3.5.2, 3.5.3, 3.5.6, 3.6.2, 3.6.3, 1.8.1, 1.5.5, 1.12.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.5 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 trails/logs and visitor sign-in sheets. Include all other CMS directed or Business Partners System Security Manual directed documents.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.	HIPAA 164.316(b)(1) HIPAA 164.316(b)(2)(ii) HIPAA 164.316(b)(2)(iii) CMS Directed ARS 10.8
Guidance: One method is to incorporate these requirements into the SSO's job description.		Related CSRs: 3.3.4, 2.2.17, 2.2.19
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.6 Retention procedures are established for all CMS sensitive information.	Review documents establishing the appropriate retention procedures.	HIPAA 164.316(b)(2)(i) CMS Directed
Guidance: Review retention procedures in relation to CMS PMs.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference
1.9.7 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.	Review documentation establishing that the required designations have been assigned with the considerations specified.	CMS Directed ARS 3.2 NIST 800-26 3.1.1
Guidance: Review the BPSSM and apply risk mitigation controls.		Related CSRs: 3.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.8 Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data verifying that vulnerability identification has been performed as specified. 3. Establish by inspection that the required summary lists are available.	PDD 63 333
Guidance: Review risk assessment.		Related CSRs: 1.8.9, 10.9.4, 1.8.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.9 The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting conduct of the required periodic reviews. 3. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.	FISCAM TSP-2.2 NIST 800-26 3.2.10 NIST 800-26 5.2 NIST 800-26 5.2.1
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.8.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.10 The system security plan establishes a security management structure with adequate independence, authority and expertise.	1. Verify by inspection that the system security plan contains the required management structure. 2. Review documentation supporting the assertion that the security management structure meets the stated requirements.	FISCAM TSP-3.1.1
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.5.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.11 Formal security and operational procedures and controls are documented.	1. Verify by inspection that the system security plan contains the required controls. 2. Review documentation supporting the security and operational controls.	NIST 800-26 12.2
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.4.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.10 Security policies shall exist that address hiring, transfer, termination, and performance.		
1.10.1 For perspective 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.	1. Inspect personnel records to confirm that references have been contacted and background checks have been performed. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documented conditions that allow access prior to completion of the screening process, as well as the in-place controls that compensate for allowing this type of access.	FISCAM TSP-4.1.1 CMS Directed NIST 800-26 6.2 NIST 800-26 6.2.4
Guidance: As part of the HR function, develop a policy and procedure to address hiring, transfer, termination, and performance items. Related CSRs: 1.1.9		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.10.2 Regular job or shift rotations are required for those personnel using sensitive information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review staff assignment records to confirm that job and shift rotations occur.	FISCAM TSP-4.1.5 FISCAM TSD-1.1.7 NIST 800-26 6.1.6
Guidance: 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. Related CSRs:		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.10.3 Regularly scheduled vacations exceeding several days are required for those personnel using sensitive information.	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.	FISCAM TSP-4.1.4 FISCAM TSD-1.1.7 NIST 800-26 6.1.6
Guidance: An approach is a policy developed that requires employees using sensitive information to take a minimum of 24 hrs continuous vacation. Related CSRs:		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.10.4 Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.	1. Review termination and transfer procedures for inclusion of the required processes. 2. 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. 3. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.	FISCAM TSP-4.1.6 HIPAA 164.308(a)(3)(ii)(C) ARS 4.2 NIST 800-26 6.1.7
Guidance: These items need to be addressed as part of a HR Termination/Transfer procedure. Related CSRs: 2.9.9, 2.2.20, 2.8.1		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement / Control Technique	Protocol	Reference
1.10.5 Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.	1. Review documentation establishing that reinvestigation policies for each position are consistent with the specified criteria. 2. Inspect personnel records to confirm sensitive position have had background reinvestigations performed within the required period.	FISCAM TSP-4.1.2

Guidance: CMS will provide future direction. Related CSRs: 2.5.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.10.6 Confidentiality or security agreements are required for CMS Business Partner Medicare employees and their contractors assigned to work with sensitive information.	1. Review policies on confidentiality or security agreements. 2. Determine whether confidentiality or security agreements are on file. 3. Review a sampling of agreements.	FISCAM TSP-4.1.3 HIPAA 164.314(a)(1) HIPAA 164.308(b)(1) HIPAA 164.308(b)(4) ARS 1.7 ARS 4.4 NIST 800-26 6.2.2

Guidance: One method would be to include the agreements as part of the procedural policy and include a standard contract clause for all procurements. Related CSRs: 1.11.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review Authorized Disclosure Agreements. 2. Review relevant policies for inclusion and directed use of the required directive.	IRS 1075 11.1@1 CMS Directed ARS 11.6

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. Related CSRs: 1.10.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 the electronically exchanged data. The CMS Business Partner will maintain a list of all contracts or other arrangements with other CMS Business Partners (include organization name and location, contract or agreement number, and purpose). The list of contracts will be provided to CMS in an MS Word document with the annual CAST submission.	1. Review documented arrangements/contracts for security content. 2. Verify risk-based decision is justified.	ARS 3.3 ARS 4.7 CMS Directed NIST 800-26 12.2.3

Guidance: A contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged should be completed prior to the exchange of data. Related CSRs: 1.5.8, 1.9.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.11.3 The CMS Business Partner has obtained satisfactory assurances that all external business associates will provide appropriate safeguards for CMS sensitive information.	1. Review the implemented safeguards. 2. Ensure satisfactory assurances have been provided.	HIPAA 164.308(b)(1) HIPAA 164.314(a)(1) ARS 10.8

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. Related CSRs: 2.14.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.11.4 Management has authorized interconnections 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.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review interconnected system agreements and established controls.	NIST 800-26 3.2.9 NIST 800-26 4.1.8

Guidance: Appropriate organizational officials should approve information system interconnection agreements. NIST SP 800-47 provides guidance on interconnecting information systems. Related CSRs: 2.14.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference

1.12 Descriptions of Medicare operations, records, and assets are validated once a year.

1.12.1	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.	Inspect the SSP and certification package for the required signatures.	CMS Directed NIST 800-26 1.2 NIST 800-26 5.1.1

Guidance: Review SSP certification package. Related CSRs: 2.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.12.2	The safeguard selection decisions and the risk assessment reports are carefully analyzed to determine whether the security requirements in place adequately mitigate vulnerabilities.	Examine documentation supporting completion of the required review.	CMS Directed NIST 800-26 1.1.6

Guidance: Review risk assessment and safeguard selection for mitigation of risks and provide recommendations. Related CSRs: 1.8.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.12.3	The CMS Business Partner is responsible for approving any necessary corrective action plans.	1. Review audit data supporting compliance with the required approval process. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. A plan of action is documented for correcting security deficiencies.	CMS Directed

Guidance: An approach is to provide annual sign-off, by senior management, on the Corrective Action Plan. Related CSRs: 1.8.7, 1.2.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	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. Review documentation supporting an assertion that the security system is fully documented. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-26 3.2.3 NIST 800-26 3.2.5

Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM. Related CSRs: 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.13 General workstation security requirements shall be established.

1.13.1	Policies and procedures are implemented that specify the proper workstation functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access CMS sensitive information.	1. Verify by inspection that the required policy/guideline is available. 2. Interview a sample to confirm familiarity with the required document.	HIPAA 164.310(b)

Guidance: One approach would be to address all the local workstations as well as the workstations used at home. Related CSRs: 7.3.3, 7.3.4, 7.3.5, 7.4.1, 7.4.2, 7.5.1, 10.6.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.13.2	Controls prohibit employees from bringing their personally owned computer equipment and software into the workplace.	1. Review the specified policy. 2. Review the controls that prohibit this.	CMS Directed NIST 800-26 10.2.13

Guidance: Bringing personal computers into the workplace creates vulnerabilities to Medicare resources and could compromise sensitive data. Related CSRs: 1.13.6, 1.13.7, 1.13.8, 2.2.28, 6.2.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.13.3 All CMS-owned software (such as CAST) 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.	1. Interview programmers and system manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming enforcement of the required process.	CMS Directed
Guidance: No further guidance required.		Related CSRs: 10.7.1, 1.13.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.4 If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the process used to assure compliance with the required policy.	CMS Directed
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.		Related CSRs: 2.2.27
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	Determine the effectiveness of controlling portable devices by review business partner mobile computing policies.	CMS Directed NIST 800-26 7.3 NIST 800-26 7.3.2
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.		Related CSRs: 2.2.27
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.6 Users are prohibited from installing desktop modems.	1. Examine user's desktops for compliance. 2. War-Dialing. 3. Review the policy on addressing desktop modems.	ARS 6.5
Guidance: If no policy currently exists, one should be created. If no process for testing exists, one should be developed.		Related CSRs: 1.13.2, 10.8.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.7 The connection of portable computing or portable network devices on the CMS claims processing network is prohibited.	Review documentation restricting the use of portable devices.	ARS 6.4
Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.		Related CSRs: 1.13.2, 1.13.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.8 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.	1. Review existing policies and procedures to ensure prohibition of modems specified. 2. Review existing procedures to ensure sampling requirement defined sufficiently to ensure adequate coverage of all assets.	ARS 6.7
Guidance: Establish a policy prohibiting the connection or use of personal modems and develop procedure to ensure testing of all assets on a recurring basis.		Related CSRs: 1.13.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference

2. *Access Control*

2.1 Audit trails/logs shall be maintained.

2.1.1	User account activity audits are conducted using automated audit controls.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the automated controls installed to implement the required process. 3. Inspect activity audit logs to confirm continuing use of the required process.	HIPAA 164.312(b) ARS 1.5 ARS 11.2 ARS 11.3 NIST 800-26 17.1.7

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 log data may be used to detect unauthorized activity and reduce volumes to manageable size.

Related CSRs: 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 4.2.1, 4.2.4, 3.1.5, 1.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. 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. 2. Review documentation establishing that the computer systems processing sensitive information are secured from unauthorized access. 3. For a sample of hardware and software security features, obtain demonstrations of feature operation. 4. Review documentation describing how audit facilities are utilized to assure that everyone accessing a computer system containing sensitive information is accountable.	HIPAA 164.310(c) IRS 1075 5.6@4.1 IRS 1075 5.6@3.3 ARS 1.1 ARS 1.5 NIST 800-26 6.1.5 NIST 800-26 8.2.1 NIST 800-26 10.2.6

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.

Related CSRs: 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 2.2.16, 2.5.1, 2.2.32

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
2.1.3 All activity involving access to and modifications of sensitive or critical files is logged.	1. Validate the types of files involved and the features are turned on or coding has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. 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 logging methodology for each of these files. 4. Inspect samples of the specified audit logs to confirm continuing use of the required process.	FISCAM TAC-4.1 ARS 1.5 ARS 11.1 NIST 800-26 16.2.5 NIST 800-26 17.1

Guidance: Access control software is used to maintain an audit trail 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.

Related CSRs: 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, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.4 Access to audit trails/logs is restricted.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required restrictions. 3. Review security software settings and compare with system security policies and procedures. 4. Inspect a sample of audit log access lists.	CMS Directed NIST 800-26 17.1.3 NIST 800-26 17.1.4

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 logs.

Related CSRs: 2.10.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.5 The audit trail includes sufficient information to establish what events occurred and who or what caused them.	1. Review a sample of event logs and audit records to confirm the required content. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed ARS 11.2 ARS 11.3 NIST 800-26 15.2.1 NIST 800-26 17.1.1 NIST 800-26 17.1.2

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.

Related CSRs: 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, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.1.6 Audit trails/logs are reviewed periodically (i.e., minimum of weekly) and retained for a minimum of 60 days.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that audit logs are being retained for the same period as the related claim. 3. Inspect a sample of audit data confirming that the required reviews have been conducted.	CMS Directed HIPAA 164.308(a)(1)(ii)(D) NIST 800-26 16.2.5 NIST 800-26 17.1.4 NIST 800-26 17.1.6
Guidance: Maintain, and periodically review, audit logs for critical application systems, including user-written applications. Audit logs may become evidence in legal proceedings, so care should be taken to protect their integrity		Related CSRs: 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, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 2.1.8
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.1.7 All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.	1. Inspect device configurations to confirm that all detected errors that can be logged are being logged. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Determine that audit logs have sufficient detail to assist with fault isolation and resolution of security abnormalities.	CMS Directed
Guidance: Audit trail 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 trail 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 trails 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.		Related CSRs: 4.1.3
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.1.8 Automated utilities are used to review audit logs daily for unusual, unexpected, or suspicious behavior. Manual reviews are performed randomly on demand, and at least once every 30 days.	1. Review audit review procedures. 2. Review audit logs. 3. Validate the system is operationally enabled.	ARS 11.5 NIST 800-26 17.1.7
Guidance: Procedures should exist which describe how to respond to an alert generated by the automated log review utilities.		Related CSRs: 2.1.6, 10.2.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

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 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. 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.	1. Review physical intrusion detection policies and procedures for spaces and rooms containing sensitive information for inclusion of the specified approach. 2. Review documentation describing measures used in conjunction with IDS to enhance protections provided directly by the IDS.	IRS 1075 4.3@24 FISCAM TAC-3.1.A.2 ARS 1.1 ARS 1.5
Guidance: Physical security controls used to detect access to facilities and protect them from intentional and unintentional loss or impairment.		Related CSRs: 3.6.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.2 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 trails and apparent security violations investigated and remedial action taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required controls. 3. Review a sample of audit data confirming consistent use of the required access process. 4. Inspect physical access audit trails to confirm that the physical accesses are being monitored.	IRS 1075 4.3@3 CMS Directed NIST 800-26 7.1.9

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.

Related CSRs: 2.8.6, 5.2.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.3 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.	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.	IRS 1075 4.3@2.2 CMS Directed

Guidance: Review BPSSM Section 4 for guidance.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.4 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.	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. Inspect a sample of audit data confirming that the secured area/perimeters are consistently secured at the end of working hours, and found secured when opened for business. 4. Confirm by inspection that the required electronic intrusion devices are in use.	IRS 1075 4.3@13 CMS Directed

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.

Related CSRs: 2.2.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.5 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.	If Security Rooms are used, review documentation confirming that each includes all of the required features.	IRS 1075 4.3@9 IRS 1075 4.3@10 IRS 1075 4.3@11 CMS Directed

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.

Related CSRs: 2.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.6 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.	IRS 1075 4.3@22 IRS 1075 4.3@23.1 IRS 1075 4.3@23.3 CMS Directed ARS 1.2

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.)

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.7 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.	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. 3. 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.	IRS 1075 4.3@1.3 CMS Directed

Guidance: Review BPSSM Section 4 for guidance.

Related CSRs: 1.1.8, 1.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.8 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.	1. Review facility security plan for procedures and policies for protection of sensitive information. 2. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of sensitive information data.	IRS 1075 4.3@19.2 IRS 1075 6.3@4 IRS 1075 4.3@19.4 CMS Directed
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.		Related CSRs: 6.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.9 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements. 3. Review documentation supporting the contention that the required process is followed for storage of sensitive information.	IRS 1075 4.3@16 CMS Directed
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.)		Related CSRs: 1.8.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.10 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.	Examine safe(s) or vault(s) for accompanying manufacturer documentation.	IRS 1075 4.3@18 CMS Directed
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.11 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of containers to confirm inclusion of the required features.	IRS 1075 4.3@15 CMS Directed
Guidance: A locked container is any metal container which is locked and to which keys and combinations are controlled.		Related CSRs: 1.8.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.12 Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.	Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.	HIPAA 164.310(c) ARS 1.1
Guidance: Workstations are located in controlled access areas and are safeguarded from unauthorized access.		Related CSRs: 2.8.6, 3.6.3, 7.3.3, 7.3.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.13 Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.	1. 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. Review documentation establishing the methods employed to deny access to sensitive information from unauthorized personnel during working hours.	HIPAA 164.310(a)(2(iii) IRS 1075 4.3@1.1 HIPAA 164.308(a)(3)(i)
Guidance: Procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.5.1, 2.5.3		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.14 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.	1. Review written emergency procedures for inclusion of the required process. 2. Inspect a sample of audit data confirming use of the required process.	FISCAM TAC-3.1.A.8 ARS 3.13 ARS 4.5 NIST 800-26 7.1.6
Guidance: Re-entry access methods are used to provide appropriate controls at emergency exits. Related CSRs: 5.6.2, 2.8.8		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.15 Procedures exist 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).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that the required process is consistently used.	HIPAA 164.312(d) HIPAA 164.308(a)(3)(i) HIPAA 164.310(a)(1) HIPAA 164.310(a)(2)(iii) ARS 3.13 ARS 7.22
Guidance: Policies and procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.4.2, 2.8.9, 2.8.3, 10.1.2		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.16 Access to facilities is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards or biometrics.	1. Review documentation designating specific individuals who are allowed access, and identifying the associated access control method used. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review a sample of audit data confirming consistent use of the required access process.	FISCAM TAC-3.1.A.3 PDD 63 711 ARS 1.1 ARS 1.3 NIST 800-26 7.1.1
Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties. Related CSRs: 1.3.15, 2.1.2, 2.5.4, 9.2.1, 2.9.4		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
2.2.17 Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of sign-in/sign-out registers to confirm collection of the required information. 3. Review a sample of audit data confirming compliance with the required register close out and review actions 4. Inspect a sample of audit data confirming monthly issue of a new AAL.	IRS 1075 4.3@4 HIPAA 164.308(a)(1)(ii)(D) HIPAA 164.310(a)(1) HIPAA 164.310(a)(2)(iii) IRS 1075 4.3@6 IRS 1075 4.3@8 HIPAA 164.312(d) FISCAM TAC-3.1.B.1 ARS 1.1 NIST 800-26 7.1.7
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.		Related CSRs: 1.9.5, 2.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.18 Management regularly reviews the list of persons with physical access to sensitive facilities.	1. Review a sample of audit data confirming periodic completion of the required reviews. 2. Review relevant policies and procedures for inclusion and directed use of the required process, and that they specify the review period.	FISCAM TAC-3.1.A.4 HIPAA 164.310(a)(2)(iii) NIST 800-26 7.1.2
Guidance: Access to sensitive facilities should be limited to personnel with a legitimate need for access to perform their duties.		Related CSRs: 2.8.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.19 Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	1. Review audit data confirming consistent use of the required procedure. 2. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.	FISCAM TAC-3.1.B.3 NIST 800-26 7.1.11
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.		Related CSRs: 1.4.1, 1.8.4, 1.9.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.20 Key combinations are changed 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.	1. Review audit data confirming consistent use of the required process. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 4.3@20.3 IRS 1075 4.3@20.6 HIPAA 164.308(a)(3)(ii)(C)
Guidance: There are 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.		Related CSRs: 1.10.4, 2.9.9, 2.8.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.21 All entry code combinations are changed periodically.	1. Review documentation and logs for entry code changes. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.1.B.2 NIST 800-26 7.1.8
Guidance: Periodically changing entry codes prevents reentry by previous employees or visitors who might have knowledge of the entry code.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
2.2.22 Unissued keys or other entry devices are secured.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.	FISCAM TAC-3.1.A.7 NIST 800-26 7.1.5

Guidance: Unissued keys and other entry devices should be stored in appropriate security containers. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.23 Keys or other access devices are needed to enter the computer room and tape/media library.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming implementation and use of the required control.	FISCAM TAC-3.1.A.5 HIPAA 164.310(a)(2)(iii) NIST 800-26 7.1.4

Guidance: Access to these areas should be limited to personnel with a legitimate need for access to perform their duties. Related CSRs: 2.8.6, 10.1.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.24 Transmission and Storage of Data - Sensitive information may only be stored on hard disk as long as the CMS Business Partner approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades and are being used. Access control devices include: (1) password security; (2) audit trails/logs; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documentation of approval and installation of the required devices. 3. Review documentation confirming that the access control devices include the required features. 4. Review audit data confirming accomplishment of the required maintenance and upgrades, 5. Review audit data confirming consistent use of the required control devices.	IRS 1075 4.7@6 CMS Directed ARS 7.13 ARS 9.2

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. Related CSRs: 5.9.6, 5.12.1, 3.6.1, 2.9.17

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.25 Handling and Transporting Bulk Sensitive Information - Care is taken to safeguard sensitive information at all times. If hand carried between facilities, it is kept with an individual and protected from unauthorized disclosure. 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."	1. Review sensitive information handling and transporting policies and procedures for control technique compliance. 2. Review sensitive information transmittal forms for accuracy and completeness. 3. Inspect a sample of sensitive information data media for labeling compliance with the requirement.	CMS Directed ARS 9.7 NIST 800-26 8.2.4 NIST 800-26 8.2.5 NIST 800-26 8.2.6

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. Related CSRs: 1.3.3, 2.5.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.26 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data supporting continuing use of the required processes.	IRS 1075 4.4 HIPAA 164.310(d)(2)(iii) ARS 9.7

Guidance: The policies and procedures for protecting and transferring sensitive information materials with receipts ensure custody control and accountability during transfers. Related CSRs: 1.3.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.27 Alternate work site equipment controls are: (1) only CMS Business Partner-owned computers and software are used to process, access, and store sensitive information; (2) 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process by personnel working from their homes or alternate worksites. 2. Inspect documentation confirming that the required controls are implemented and consistently used.	IRS 1075 4.7@2 IRS 1075 4.7@3 IRS 1075 4.7@4.1 IRS 1075 4.7@5 CMS Directed

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. Related CSRs: 1.13.4, 1.13.5

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.

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.28 Responsibility is assigned and security procedures are documented for bringing 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.	Inspect documentation confirming that the required controls are implemented and consistently used.	HIPAA 164.310(d)(1) HIPAA 164.310(d)(2)(iii)

Guidance: The procedures for checking all hardware and software in to and out of the facility assist in maintaining an accurate inventory. Related CSRs: 1.13.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.29 Procedures are implemented to control access to software programs undergoing testing or revision.	Procedures are in place to protect CMS sensitive information during software testing and revisions.	HIPAA 164.310(a)(2)(iii)

Guidance: It is good practice to have an Security Test and Evaluation plan. Related CSRs: 6.4.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.30 Policies and procedures are implemented to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).	A maintenance tracking system should be implemented.	HIPAA 164.310(a)(2)(iv)

Guidance: It is a good practice to keep an inventory of resources. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.31 Boot access to removable media drives is disabled when not explicitly required. Removable media drives are removed when not explicitly required. System BIOS settings are locked and BIOS access is password-protected.	1. Review system configuration logs. 2. Examine access audit logs. 3. Randomly validate BIOS access is protected on desktops. 4. Review documentation on authorized removable media.	ARS 7.14

Guidance: Access to removable media drives should be tightly controlled. BIOS access should also be controlled. Related CSRs: 1.3.14, 1.5.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.32 Physical ports (e.g., wiring closets, patch panels, etc.) are disabled when not in use.	Review documentation requiring the disabling of physical ports.	ARS 1.10
Guidance: Policy should exist which defines the physical ports that are required for operation.	Related CSRs: 2.1.2, 2.3.2	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	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.	FISCAM TAC-3.2.B
Guidance: It is important that all access paths (e.g., Internet, dial-in, telecommunications) be identified and controlled to eliminate "backdoor" paths.	Related CSRs: 3.4.1, 4.5.1, 2.3.2, 10.8.6	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.3.2 All proxies not explicitly required are disabled and/or removed. Proxy access is granted only to those hosts, ports, and services that are explicitly required.	1. Review list of hosts, ports, and services to which proxy access is granted. 2. Review the policy statement.	ARS 6.3
Guidance: Hosts, ports, and services that are required should be explicitly identified.	Related CSRs: 2.3.1, 2.2.32	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review documentation of the access control process to confirm inclusion of a procedure for emergency access. 2. Review documentation of the access control process to confirm inclusion of at least one of the required features.	HIPAA 164.312(a)(2)(ii) HIPAA 164.310(a)(1) HIPAA 164.312(a)(2)(i) ARS 5.5
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.	Related CSRs: 5.2.7, 5.6.2, 2.9.12	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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 and; (4) automatically terminated after a predetermined period.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that all four specified elements of the required process is consistently used.	FISCAM TAC-2.2 ARS 4.5 NIST 800-26 15.1.4
Guidance: As with normal access authorizations, emergency and temporary access should be approved and documented.	Related CSRs: 5.2.7, 2.2.15, 2.8.3, 2.8.9	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	1. Inspect documentation identifying systems that process sensitive information. 2. Review documentation establishing that all computers in all specified systems meet requirements in their implemented configuration. 3. Review documentation of the configuration management process used to assure that all systems remain in certified configurations.	IRS 1075 5.7@2 CMS Directed
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.		Related CSRs: 2.2.13, 1.9.1, 2.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.2 Classifications and criteria have been established and communicated to resource owners.	1. Review policies specifying classification categories and related criteria to be used by resource owners in classifying their resources according to the need for protective controls. 2. Inspect audit data confirming that the required policy has been communicated to resource owners.	FISCAM TAC-1.1
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.		Related CSRs: 1.7.1, 2.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.3 Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation establishing that existing safeguards provide the required protections.	HIPAA 164.312(d) IRS 1075 6.3@7.1 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) PDD 63 711 ARS 7.22 ARS 10.8
Guidance: Policies and procedures limit access while ensuring that properly authorized access is allowed based on an employee's need-to-know.		Related CSRs: 2.12.1, 2.2.13, 2.7.2, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.4 Sensitive information is kept separate from other information to the maximum extent possible. Files are clearly labeled to indicate that sensitive information is included. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information.	1. Review sensitive information handling procedures for inclusion of the required processes. 2. For a sample of media and devices containing sensitive information, inspect to confirm use of the required labels.	IRS 1075 5.3@1.1 IRS 1075 5.3@2.1 IRS 1075 5.3@3.1 IRS 1075 5.3@3.2 CMS Directed ARS 9.3 NIST 800-26 8.2.5
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 log 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.		Related CSRs: 2.2.16, 1.3.15, 2.2.25
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.5.5 Every personnel position with access to CMS sensitive information processing is designated with a sensitivity level, and documentation is available to support the security and suitability standards for these personnel commensurate with their position sensitivity level and appropriate personnel investigation requirements.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample of personnel positions, inspect documentation establishing the associated sensitivity level.	CMS Directed PDD 63 711 NIST 800-26 6.1.1
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.		Related CSRs: 1.10.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.6 An 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 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 documentation verifying independent review includes interconnect system security controls.	IRS 1075 6.3@7.2 FISCAM TSP-5.1.2 NIST 800-26 2.1 NIST 800-26 2.1.1 NIST 800-26 2.1.2 NIST 800-26 3.2.6
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.		Related CSRs: 1.8.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.7 CMS Business Partner office facilities processing sensitive information are subjected to an annual self-assessment.	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.	CMS Directed IRS 1075 6.3@7.2 FISCAM TSP-5.1.1
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.		Related CSRs: 2.12.1, 1.4.2, 1.8.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.8 Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.	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.	HIPAA 164.316(b)(2)(i) IRS 1075 6.3@7.3.1 CMS Directed
Guidance: Inspection, self-assessment, and corrective action reports are an important means of identifying areas of noncompliance and remedial actions performed to correct noncompliance.		Related CSRs: 1.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.9 Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.	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.	CMS Directed IRS 1075 5.6@8
Guidance: The procedures are used to test the security system attributes.		Related CSRs: 1.4.2, 5.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.5.10 Sensitive information system development documentation is available, including security mechanisms and implementation.	Inspect system design and test documentation for an explanation of security mechanisms and how they are implemented.	FISCAM TCC-1.1.1

Guidance: The system development documentation provides security mechanism and implementation review guidance to staff with varying levels of skill and experience. Related CSRs: 6.3.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.5.11 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.	Review the sensitive information system documentation for inclusion of required test documentation.	FISCAM TCC-2.1.1 FISCAM TCC-2.1.4 FISCAM TCC-2.1.8 NIST 800-26 12.1.5

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. Related CSRs: 6.3.1, 6.3.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.6 Actual or attempted unauthorized, unusual, or sensitive access shall be monitored.

2.6.1 Security violations and activities, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.	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.	FISCAM TAC-4.2 ARS 10.6 ARS 11.1 NIST 800-26 11.2.6 NIST 800-26 16.1.10 NIST 800-26 17.1 NIST 800-26 17.1.8

Guidance: Audit functions should be activated to maintain critical audit trails and report unauthorized or unusual activity to the appropriate personnel. Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 4.2.1, 4.2.4, 3.1.1, 10.2.3, 2.9.1, 10.2.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.6.2 Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.	1. Review documentation of the controls used to enforce this requirement. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed

Guidance: Audit trails 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 trail that logs 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 recorded in an audit log. Related CSRs: 3.6.5, 5.2.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Confirm by inspection that the required procedures exist. 2. By inspection confirm that supervisors have specified procedures.	CMS Directed

Guidance: Procedures should be in-place to monitor visitors and contractors to insure they perform only authorized activities and work functions. Related CSRs: 2.2.17

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	1. Review resource classification documentation and compare to risk assessments. 2. Inspect audit data confirming that the required approval and review processes are consistently used.	FISCAM TAC-1.2 PDD 63 711
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.		Related CSRs: 1.7.1, 2.5.2, 1.8.3, 4.4.1, 1.12.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	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.	IRS 1075 5.2@1.1 HIPAA 164.308(b)(1) HIPAA 164.308(a)(4)(ii)(C) IRS 1075 5.2@1.3 CMS Directed HIPAA 164.308(a)(4)(i) ARS 4.4 ARS 7.22
Guidance: The policies and procedures for limiting access ensure that properly authorized access is allowed based on an employee's need-to-know.		Related CSRs: 2.12.1, 2.5.3, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8 Resource owners shall identify authorized users and the level of authorization.		
2.8.1 Security is notified immediately when system users are terminated or transferred.	1. Review relevant policies and procedures for inclusion and directed use of the required procedure. 2. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.	FISCAM TAC-2.1.6
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.		Related CSRs: 1.10.4, 2.2.20, 2.9.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.2 All changes to security profiles by SSO or designated representative are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming routine identification and investigation of unusual activity. 3. Review a selection of recent profile changes and activity logs.	FISCAM TAC-2.1.5
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.		Related CSRs: 9.3.4, 2.11.4, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.3 SSOs or their designated representative review access authorizations and discuss any questionable authorizations with resource owners.	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.	FISCAM TAC-2.1.4 PDD 63 711 ARS 7.22
Guidance: One method is for a listings of authorized users and their specific access needs should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security manager.		Related CSRs: 1.4.1, 2.2.15, 2.4.2, 3.3.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement / Control Technique	Protocol	Reference
2.8.4 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a selection of users with dial-up access, review authorization and justification.	FISCAM TAC-2.1.3 ARS 7.11
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.		Related CSRs: 10.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
2.8.5 Owners periodically review access authorization listings and determine whether they remain appropriate.	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.	FISCAM TAC-2.1.2 PDD 63 711 NIST 800-26 15.2.2
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.		Related CSRs: 2.2.18, 1.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.6 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.	1. By inspection, confirm that authorization lists include the required information. 2. Inspect audit data confirming continuing maintenance of authorization lists and access controls for restricted areas.	CMS Directed
Guidance: Authorization lists and controls for restricted areas should be part of doing business to restrict access to areas containing or processing sensitive information.		Related CSRs: 6.4.1, 2.2.2, 2.2.12, 2.2.23
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.7 Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample representing each type of computer operating system, and for standalone and each mode of network connection affecting banner display, observe that the warning banner on the sample computer is consistent with the documented procedure.	IRS 1075 5.1@1.3 CMS Directed ARS 3.6
Guidance: The log-on banner/screen warning banner warns the user that the system processes sensitive information and it is subject to monitoring each time they log-on.		Related CSRs: 10.8.3, 10.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.8 Documented policies and procedures exist 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.	Review the appropriate documented policies and procedures for inclusion of the required rules.	HIPAA 164.312(a)(1) HIPAA 164.312(e)(1) HIPAA 164.308(a)(3)(i) ARS 4.5 ARS 11.7
Guidance: The policies and procedures used to grant different levels of access to sensitive information are based on an employee's need-to-know.		Related CSRs: 2.2.14
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.8.9 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to the SSO.	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.	FISCAM TAC-2.1.1 NIST 800-26 15.1.1

Guidance: Policies and procedures should exist for authorizing access to information resources and for documenting such authorizations. Related CSRs: 2.14.1, 2.2.15, 1.4.1, 2.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.1 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 administrative reset.	1. Review security software password parameters. 2. Review pertinent policies and procedures. 3. Observe the system directed action in response to four invalid access attempts, confirming that the action is consistent with the documented policy.	FISCAM TAC-3.2.A.5 ARS 7.12 NIST 800-26 15.1.14

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. Related CSRs: 2.6.1, 7.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.2 Use of names or words as passwords is prohibited.	Review relevant policies for inclusion and directed use of the required prohibition.	FISCAM TAC-3.2.A.2

Guidance: 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. Related CSRs: 1.1.1, 3.6.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.3 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.	1. Interview a sample of users to confirm the required understanding and device possession. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.8

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. 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). 3. Review documentation describing audit systems implemented to record all accesses, including access scripts, to protected information. 4. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description. 5. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing. 6. Inspect a sample of access audit data supporting continuing use to the required process.	HIPAA 164.312(e)(1) IRS 1075 4.7@6 FISCAM TAC-3.2.A HIPAA 164.312(a)(1) ARS 9.2 NIST 800-26 15.1.3

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.

Related CSRs: 2.7.2, 2.2.16, 2.5.3, 2.11.4, 7.4.1, 7.4.2, 2.9.14

☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***

2.9.5 When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) Authentication is provided through ID 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.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. 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.)
3. 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.
4. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.

IRS 1075 5.8@5.1
IRS 1075 5.8@5.2
IRS 1075 5.8@5.3
IRS 1075 5.8@5.4
FISCAM TAC-3.2.E.1
ARS 7.1
ARS 7.11
NIST 800-26 16.2.4

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.

Related CSRs: 3.6.1, 3.6.3, 10.8.2, 10.10.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.6 Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff after a predetermined amount of time (normally 15 minutes) and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), or (d) telephone callback procedure.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation supporting implementation of the required controls.
3. Review a sample of audit data confirming continuing use of the required controls.

HIPAA 164.312(a)(2)(iii)
HIPAA 164.312(d)
HIPAA 164.312(a)(2)(i)
ARS 1.1
ARS 7.1
ARS 7.15
ARS 7.16
ARS 7.21
NIST 800-26 15.1

Guidance: Procedures should be in place to authenticate users before granting them access to the system or application.

Related CSRs: 7.3.5, 10.8.2, 10.10.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.7 Password files are encrypted.

1. View a sample dump of password files (e.g., hexadecimal printout).
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM TAC-3.2.A.7

Guidance: Encrypting the password file reduces the risk that it could be accessed and read by unauthorized individuals.

Related CSRs: 10.5.1, 2.9.16, 2.9.17

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
2.9.8 Vendor-supplied passwords are replaced immediately.	1. 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. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.3 NIST 800-26 15.1.13

Guidance: Vendor supplied passwords are known by every hacker and they are usually the first passwords tried by hackers. Related CSRs: 3.6.2, 10.10.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.9 Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	1. Review pertinent policies and procedures. 2. Review documentation of such comparisons. 3. Interview security managers. 4. Make comparison using audit software.	FISCAM TAC-3.2.A.6 NIST 800-26 15.1.5

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. Related CSRs: 1.10.4, 2.2.20, 2.8.1, 2.10.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.10 Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed every 60 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least 8 characters in length; (6) must include at least one number, one upper/lower case character, and one special character; and (7) prohibited from reuse for at least 6 generations.	1. Interview users. 2. Review security software password parameters. 3. Observe users keying in passwords. 4. Attempt to log on without a valid password. Make repeated attempts to guess passwords. 5. Assess procedures for generating and communicating passwords to users. 6. Review pertinent policies and procedures.	FISCAM TAC-3.2.A.1 CMS Directed HIPAA 164.308(a)(5)(ii)(D) FISCAM TAC-3.2.A.4 ARS 3.9 ARS 3.10 ARS 3.11 NIST 800-26 15.1.6 NIST 800-26 15.1.7 NIST 800-26 15.1.9

Guidance: Policies and procedures should exist that implement these minimum password requirements. Related CSRs: 7.3.2, 10.10.1, 2.9.14

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.11 Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. 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.	1. Inspect a sample of workstations running each type of operating system in use to confirm that the required process is in use. 2. Review configuration documentation supported implementation of the required feature.	FISCAM TAC-3.2.C.3 CMS Directed HIPAA 164.310(b) ARS 7.15 ARS 7.16 NIST 800-26 16.1.4

Guidance: Workstation 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. Related CSRs: 7.3.5, 10.10.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.12 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.	Review documentation establishing that authorization control exists, and includes the required feature.	HIPAA 164.308(a)(4)(ii)(B) ARS 11.6

Guidance: The mechanisms are used to authenticate users before granting them access permissions to the system or application. Related CSRs: 2.4.1, 2.9.18

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.9.13 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.	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.	HIPAA 164.308(a)(4)(ii)(A)
Guidance: Review security policies and procedures for business partner access.		Related CSRs: 1.4.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.14 System Administrators use unique UserIDs and passwords to perform administrator functions. These UserIDs are not shared with anyone and are different from the administrator's own personal UserID.	1. Ensure that System Administrators have unique UserID when performing admin functions. 2. Interview System Administrators regarding their UserIDs 3. Review usage reports to establish activity.	ARS 3.12
Guidance: Available procedures define the usage of the unique UserIDs.		Related CSRs: 2.9.10, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.15 Unique and separate administrator accounts are used for administrative versus non-administrative activities.	1. Ensure that System Administrators have unique UserID when performing admin functions. 2. Interview System Administrators regarding their UserIDs.	ARS 7.7
Guidance: The use of unique and separate accounts helps to ensure that administrative activities are kept separate from non-administrative activities.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.16 Highly sensitive system files are encrypted.	1. Verify that the designated files have been encrypted. 2. Develop criteria for identification of files that should be encrypted	ARS 7.18
Guidance: Encryption of sensitive system files helps ensure that file access is limited. The encryption feature should be evaluated, implemented, and tested for protecting sensitive files. Highly sensitive system files may include, but are not limited to, password files, digital signature private keys, or other Business Partner-designated sensitive files.		Related CSRs: 2.9.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.17 Data are protected with system access controls and encrypted when residing in non-secure areas.	Review documentation confirming that the controls and encryption features are properly implemented in non-secure areas.	ARS 9.1 NIST 800-26 7.3.1
Guidance: The robustness of protection provided should be commensurate with the sensitivity of the information.		Related CSRs: 2.2.24, 2.9.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.18 User identification is required for any transaction that has information security implications.	1. Review helpdesk procedures. 2. Interview helpdesk personnel to verify understanding of requirement.	ARS 3.5
Guidance: Help desk policy should require individual identification before transactions can be completed.		Related CSRs: 2.9.12, 1.1.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.19 Controls are in place to determine compliance with password policies.	Review the procedures for determining compliance with password policies.	NIST 800-26 11.2.3
Guidance: Procedures should exist to ensure compliance with password policies through review or testing.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.9.20 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.	1. Review the policies and procedures for distributing passwords. 2. Review the policies and procedures for handling lost and compromised passwords.	NIST 800-26 15.1.10 NIST 800-26 15.1.11

Guidance: Users take reasonable measures to safeguard passwords, including not loaning or sharing passwords with others, and reporting lost or compromised passwords immediately.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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. Access to security software is restricted to security administrators only.	1. Review documentation describing the security software in use for restriction of access to data files and software programs. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of security software parameters that limit access to the security software to security administrators.	FISCAM TAC-3.2.C.1 FISCAM TAC-3.2.C.2 ARS 7.22 NIST 800-26 16.1.3

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.

Related CSRs: 3.6.4, 3.6.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Perform penetration testing by attempting to access and browse computer resources. 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. 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. 5. Review documentation describing the standardized naming conventions in use for resources.	FISCAM TAC-3.2.C.5 FISCAM TAC-3.2.C.6 ARS 7.9 NIST 800-26 16.1.2 NIST 800-26 16.1.6

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.

Related CSRs: 6.4.3, 6.4.4, 2.1.4, 3.6.5, 6.4.1, 6.8.2, 2.10.6

☐ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
2.10.3 Modification of data is restricted to authorized employees.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List(s) identifying employees who are authorized to update data. 3. Inspect a sample of audit data confirming that the required process is consistently used 4. Review documentation of the control used to restrict of data updating to authorized employees.	CMS Directed
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.		Related CSRs: 7.4.1, 7.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review documentation of the process used to provide the specified control over routines that modify the status of a file. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.	CMS Directed
Guidance: Utilities for file access and related processing need controls in place.		Related CSRs: 7.4.1, 7.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.10.5 Inactive user accounts are monitored and removed when not needed.	1. Review a sample of audit data confirming continued operation of the required control. 2. Review documentation describing how the required control is implemented.	FISCAM TAC-3.2.C.4 NIST 800-26 15.1.8 NIST 800-26 16.1.5
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.		Related CSRs: 2.9.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.10.6 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.	1. Validate security program system setup or rules (RAC-F/ACF2/TopSecret) or access setup in other operating systems. 2. Examine access in system audit logs.	ARS 7.3 NIST 800-26 16.3
Guidance: It is important that the OS controls are implemented to disable public read and write access to sensitive information.		Related CSRs: 1.9.3, 2.10.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.11 Logical controls shall be implemented for databases and DBMS software.		
2.11.1 Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	1. Review security system parameters. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.D.4
Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.11.2 Access and changes to DBMS software are controlled.	1. Review the controls protecting DBMS software. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.D.3 HIPAA 164.310(a)(2)(iii)

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.

Related CSRs: 6.5.2, 6.6.1, 3.4.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.11.3 Use of DBMS utilities is limited.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List for DBMS utilities to confirm access is limited to those personnel have an operational requirement for access.	FISCAM TAC-3.2.D.2

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 trails.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.11.4 Database management systems (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) control access to the data dictionary using security profiles and passwords; (3) maintain audit trails/logs that allow monitoring of changes to the data dictionary; and (4) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.	1. Interview database administrator. 2. Test controls by attempting access to restricted files. 3. Review pertinent policies and procedures.	FISCAM TAC-3.2.D.1 ARS 11.2 ARS 11.3 NIST 800-26 16.1.9

Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. Data dictionary software, which interfaces with the DBMS and provides a method for documenting elements of a database, may also provide a method of securing data. In addition, use of the DBMS and data dictionary should be protected through the use of logical access controls and audit trails.

Related CSRs: 6.3.5, 6.6.1, 2.8.2, 2.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	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.	IRS 1075 6.3@5 PDD 63 193 ARS 3.2

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.

Related CSRs: 1.4.2, 2.5.3, 2.5.7, 2.7.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.12.2 Medicare data are not released to outside personnel unless the personnel are authorized to receive the data and their identity is verified.	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.	CMS Directed

Guidance: There should be procedures used to verify that outside personnel who request Medicare data are authorized to receive the data before releasing it.

Related CSRs: 1.3.2, 1.3.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.	FISCAM TAC-4.3.1 FISCAM TAC-4.3.2 NIST 800-26 7.1.10
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.		Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.13.2 Violations are summarized and reported to senior management.	1. Interview senior management and personnel responsible for summarizing violations. 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.	FISCAM TAC-4.3.3
Guidance: 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.		Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.13.3 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	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.	FISCAM TAC-4.3.4
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.		Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.2, 3.1.1, 3.4.1, 1.2.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.13.4 Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.	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.	IRS 1075 3.2@2.4 CMS Directed
Guidance: The process of inventorying and documenting missing tapes containing sensitive information should be integrated into the normal business processes of the organization.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect standard approval forms.	FISCAM TAC-2.3.1
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.		Related CSRs: 1.3.8, 2.8.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

2.14.2 Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Protocol: Examine documents authorizing file sharing and file sharing agreements.

Reference: FISCAM TAC-2.3.2; NIST 800-26 16.2.7

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.

Related CSRs: 1.11.3, 1.11.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.

Protocol: Review system operational policies and guidelines.

Reference: FISCAM TSS-2.2.2; NIST 800-26 11.2.2

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.

Related CSRs: 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 2.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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).

Protocol: Determine when the last management review was conducted, and analyze their review regarding the intended functioning of software monitoring control techniques and controlling risk.

Reference: FISCAM TSS-2.2.4; ARS 7.5

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.

Related CSRs: 6.3.10, 1.5.5, 1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.9.7, 2.13.3, 4.4.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.1.3 The use of privileged system software and utilities is reviewed by technical management.

Protocol:
1. Interview technical management regarding their reviews of privileged system software and utilities usage.
2. Review documentation supporting technical management reviews.
3. Review documentation for system software utilities and verify that technical management has given use approvals.
4. 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 user ID`s for performing privileged and normal activities? - Are the login privileges for highly privileged accounts available only from console and terminals situated within the console room ? - Is the audit trail maintained of activities conducted by highly privileged users? How long is it preserved?

Reference: FISCAM TSS-2.2.1; ARS 7.4

Guidance: Privileged access may be used only to perform assigned job duties.

Related CSRs: 1.8.4, 3.3.3, 4.1.3, 4.3.1, 4.6.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***System Software***

General Requirement / Control Technique	Protocol	Reference
3.1.4 Systems programmers' activities are monitored and reviewed.	1. Determine that system programmer supervisors are supervising and monitoring their staff. 2. Review documentation supporting the supervising and monitoring of systems programmers' activities. 3. 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.	FISCAM TSS-2.2.3 ARS 7.6 ARS 7.8

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 logon 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.

Related CSRs: 4.2.1, 4.2.4, 3.2.3, 4.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.1.5 Systems support alarm features to provide immediate notification of predefined events.	1. Review security plan to determine use of audit logs and alarms set points. 2. Review audit logs.	HIPAA 164.312(b)

Guidance: It is a good practice to have an automated audit system perform the immediate notification.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Verify that the appropriate responsibilities have been defined. 2. Interview systems programmers regarding their responsibilities.	FISCAM TSS-2.1.2 NIST 800-26 10.1.5

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.

Related CSRs: 1.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.2.2 Responsibilities for monitoring use are defined and understood by technical management.	1. Verify that the appropriate responsibilities are defined. 2. Interview technical management regarding their responsibilities.	FISCAM TSS-2.1.3

Guidance: Security training is adjusted to the level of the technical management's responsibilities.

Related CSRs: 1.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.2.3 Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	1. Interview management and systems personnel. 2. Verify the existence and current version of the appropriate policies and procedures.	FISCAM TSS-2.1.1

Guidance: 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.

Related CSRs: 3.1.4, 4.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
3.2.4 The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	1. Determine whether logging occurs and what information is logged. 2. Review logs. 3. Using security software reports, determine who can access the logging files.	FISCAM TSS-2.1.4 NIST 800-26 10.1.5

Guidance: The output report log 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. Related CSRs: 1.9.4, 9.6.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review pertinent policies and procedures. 2. Interview management and system personnel regarding access restrictions. 3. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. 4. Attempt to access the operating system and other system software.	FISCAM TSS-1.1.2

Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses. Related CSRs: 1.1.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.3.2 Policies and procedures for restricting access to systems software exist and are up-to-date.	1. Interview management and systems personnel regarding access restrictions. 2. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. 3. Attempt to access the operating system and other system software. 4. Review pertinent policies and procedures.	FISCAM TSS-1.1.1

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. Related CSRs: 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of system programmers were reviewed.	FISCAM TSS-1.1.4

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 logs. 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. Related CSRs: 3.1.3, 1.1.2, 2.8.3, 4.6.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.3.4 Justification and management approval for access to systems software is documented and retained.	1. Interview system manager and security administrator. 2. Review appropriate documentation, and verify that it is retained.	FISCAM TSS-1.1.3

Guidance: 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. Related CSRs: 1.9.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***System Software***

General Requirement Control Technique	Protocol	Reference
3.4 Installation of system software shall be documented and reviewed.		
3.4.1 Installation of all system software is logged to establish an audit trail/log and is reviewed by data center management.	1. Interview data center management about their role in reviewing system software installations. 2. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.	FISCAM TSS-3.2.4
Guidance: A good process for monitoring and documenting migration of system software is in the change management process for the organization.	Related CSRs: 9.7.1, 9.8.1, 9.8.2, 9.8.3, 6.5.2, 2.3.1, 2.11.2, 2.13.3, 4.7.6, 6.3.5, 6.3.6, 6.3.10, 6.6.1, 6.7.1, 6.8.1, 10.7.3, 10.10.1	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.4.2 Migration of tested-and-approved system software to production use is performed by an independent library control group.	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.	FISCAM TSS-3.2.2
Guidance: A good process for monitoring and documenting the migration of system software is in the change management process for the organization.	Related CSRs: 6.8.2, 4.7.6	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.4.3 Vendor-supplied system software includes software documentation and is supported by the vendor.	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.	FISCAM TSS-3.2.5 NIST 800-26 12.1.1 NIST 800-26 12.1.2
Guidance: A good approach is to include vendor maintenance with the purchase of the software.	Related CSRs:	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.4.4 Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	1. Interview management and systems programmers about scheduling and giving advance notices when system 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.	FISCAM TSS-3.2.1
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.	Related CSRs: 5.9.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement / Control Technique	Protocol	Reference
3.4.5 Outdated versions of system software are removed from production libraries.	Review supporting documentation from a few system software migrations and the removal of outdated versions from production libraries.	FISCAM TSS-3.2.3

Guidance: 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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.4.6 All system software is current and has current and complete documentation.	1. Review documentation and test whether recent changes are incorporated. 2. Interview management and system programmers about the currency of system software, and the currency and completeness of software documentation.	FISCAM TSS-3.2.6

Guidance: An automated version tracking system can assist with tracking the current version of software and the software's documentation.

Related CSRs: 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.5 System software changes shall be authorized, tested and approved before implementation.

3.5.1 New system components and software versions or products and modifications to existing system software are tested and the test results are approved before implementation.	1. Determine the procedures used to test and approve system components and software prior to its implementation. 2. Select a few recent system component and software changes and review audit data confirming that the specified process was followed. 3. Review procedures used to control and approve emergency changes. 4. Select some emergency changes to system components and software, and test whether the indicated procedures were used.	FISCAM TSS-3.1.4 NIST 800-26 10.2 NIST 800-26 10.2.2

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.

Related CSRs: 5.7.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Interview management and systems personnel. 2. Verify that policies and procedures are current, and contain the required information. 3. Review the mission/business impact analysis documentation.	FISCAM TSS-3.1.1 NIST 800-26 1.2.2 NIST 800-26 10.2.1

Guidance: Usually, the change request will contain most of the selection, installation, modification, and cost information.

Related CSRs: 1.9.4, 1.4.1, 1.8.4, 4.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement Control Technique	Protocol	Reference
3.5.3 Procedures exist for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.	1. Review procedures for identifying and documenting system software problems. 2. Interview management and systems programmers. 3. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.	FISCAM TSS-3.1.2
Guidance: A good approach is to automate the software problem tracking processes. Monthly tracking reviews will assist in controlling any issues.		Related CSRs: 1.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.5.4 New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.	1. Determine what authorizations and documentation are required prior to initiating system software changes. 2. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.	FISCAM TSS-3.1.3
Guidance: A preformatted change request process provides efficiency and assists in the accuracy of the change tracking processes.		Related CSRs: 6.6.1, 6.7.1, 4.7.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.5.5 Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.	Verify the existence of checkpoint and restart capabilities.	CMS Directed
Guidance: Checkpoints and Restart capabilities on jobs will assist in meeting performance goals.		Related CSRs: 4.7.6
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.5.6 Procedures exist 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.	1. Interview an independent IT supervisor who has previously reviewed changes. 2. Verify the existence of emergency change procedures. 3. Interview system managers.	FISCAM TSS-3.1.5
Guidance: A good approach is to include emergency procedures in the change management process as well as appropriate procedures in the Contingency Plan		Related CSRs: 5.6.2, 5.7.2, 6.6.1, 1.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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 logged by automated logging facilities.	Review sample accesses to system software files to confirm automated logging facilities.	FISCAM TSS-1.2.2
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 logging or file changes occur.		Related CSRs: 2.2.24, 2.9.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.6.2 All vendor-supplied default logins, passwords, and security parameters have been disabled or reinitialized to more secure settings.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Test for default presence using vendor standard IDs and passwords.	FISCAM TSS-1.2.3 ARS 7.2 NIST 800-26 16.2.12 NIST 800-26 16.2.3
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.		Related CSRs: 2.9.8, 1.9.4, 10.10.1, 2.9.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***System Software***

General Requirement Control Technique	Protocol	Reference
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.	1. Determine what terminals are set up as master consoles and what controls exist over them. 2. 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.	FISCAM TSS-1.2.4

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.

Related CSRs: 1.9.4, 2.2.12, 2.9.5, 10.10.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Obtain a list of all system software on test and production libraries used by the entity. 2. Verify that access control software restricts access to system software. 3. Using security software reports, determine who has access to system software files, security software, and logging files. Reports should be generated by the auditor, or at least in the presence of the auditor. 4. 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.	FISCAM TSS-1.2.2 HIPAA 164.310(a)(2)(iii)

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.

Related CSRs: 2.10.1, 1.1.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.6.5 The operating system is configured to prevent circumvention of the security software and application controls.	1. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods. 2. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.	FISCAM TSS-1.2.1 NIST 800-26 10.1.4

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.

Related CSRs: 2.10.1, 2.10.2, 2.2.1, 2.6.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.6.6 The operating system's operational status and restart integrity is protected during and after shutdowns.	1. Interview the system manager. 2. Verify the protection of the operating system during and after shutdowns.	CMS Directed

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.

Related CSRs: 5.2.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
3.6.7 All system defaults are reset after being restored from a backup.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify through testing or procedure reviews that system defaults are reset after being restored from a backup.	NIST 800-26 9.2.8

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.

Related CSRs: 5.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4. *Segregation of Duties*

4.1 Formal procedures shall guide personnel in performing their security duties.

4.1.1 Application-run manuals provide instruction on operating specific applications, including in-house applications.	1. Inspect run manuals for inclusion of the required instructions. 2. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-3.1.3 NIST 800-26 12.1.3

Guidance: Manuals should include instructions on job setup, console and error messages, job checkpoints, transaction logs, and restart and recovery steps after system failure.

Related CSRs: 4.1.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.1.2 Operators are prevented from overriding file labels or equipment error messages.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing how controls meet the specified requirement. 3. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-3.1.4

Guidance: A good approach is to provide periodic training in operating procedures, which should cover operator-prohibited activities.

Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.1.3 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.	1. Determine that the required operator and security manuals exist, and that they provide the required documentation. 2. Determine that documents are understood and adhered to by staff.	FISCAM TSD-3.1.2 NIST 800-26 12.1 NIST 800-26 12.1.7

Guidance: Manuals should contain instructions on all procedures which the employee is expected to perform on a regular basis and in an emergency situation.

Related CSRs: 5.6.2, 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 4.1.1, 3.1.3, 3.1.5, 2.1.7, 4.2.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.1.4 The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing use of the specified approval process.	CMS Directed

Guidance: The approval process should be documented and reviewed periodically.

Related CSRs: 3.5.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Segregation of Duties***

General Requirement / Control Technique	Protocol	Reference
4.1.5 Duties in critical or sensitive control and financial functions are split to ensure least privileged and individual accountability.	1. Interview supervisors in the critical and sensitive control and financial areas. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-26 6.1 NIST 800-26 6.1.3

Guidance: Duties should be documented in job descriptions. Appropriate separation of data will assist in preventing fraud. See BPSSM information on fraud protective measures.

Related CSRs: 4.3.1, 4.7.2

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.2 Active supervision and review shall be provided for all personnel.

4.2.1 All operator activities on the computer system are recorded on an automated history log.	1. Determine by review that an automated history log exists on each computer system, and that they record all operator activities. 2. Interview supervisors to confirm that supervisors routinely review history log.	FISCAM TSD-3.2.2

Guidance: The history log serves as an audit trail and should be reviewed routinely by supervisors.

Related CSRs: 2.1.1, 2.6.1, 3.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.2.2 Personnel are provided adequate supervision and review, including each shift of computer operations.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing supervision and review in accordance with the documented process.	FISCAM TSD-3.2.1

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.

Related CSRs: 1.4.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Interview supervisors and subordinate personnel to confirm continuing use of the required process. 2. Observe system startup. 3. Review audit data confirming that only authorized personnel are involved in the system startup operation. 4. Review audit data confirming that parameters set during IPL are consistently in accordance with documented procedures.	FISCAM TSD-3.2.4

Guidance: IPL establishes the environment in which the computer operates. System startup should be monitored to ensure that security features are enabled.

Related CSRs: 4.1.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.2.4 Supervisors routinely review the history log and investigate any abnormalities.	1. Determine, by review supervisor's job description that this is included in the job description. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review history log for signatures indicating supervisory review. 4. Inspect a sample of documentation of the supervisor's investigative process.	FISCAM TSD-3.2.3

Guidance: The history log serves as an audit trail.

Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 2.1.1, 2.6.1, 3.1.4, 3.1.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Segregation of Duties***

General Requirement / Control Technique	Protocol	Reference
4.3 Job descriptions shall be documented.		
4.3.1 Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	1. Review documentation establishing that existing documented job descriptions meet segregation of duty principles. 2. Inspect the effective dates of position descriptions to confirm that they are current. 3. Confirm by interview of the incumbents that documented job descriptions match actual current responsibilities and duties.	FISCAM TSD-1.2.1 NIST 800-26 6.1.2
Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.		Related CSRs: 3.1.3, 4.1.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Confirm by review that job descriptions are documented, and that they meet the specified criteria. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSD-1.2.2
Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.		Related CSRs: 5.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.4 Management shall review 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).	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.	FISCAM TSD-2.2.2
Guidance: A good approach is a documented management review on an annual basis.		Related CSRs: 3.1.2, 2.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.4.2 Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.	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.	FISCAM TSD-2.2.1
Guidance: A periodic employee performance review could be used to demonstrate compliance.		Related CSRs: 3.1.4, 3.2.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.5 Physical and logical access controls shall be established.		
4.5.1 Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	Review documentation establishing now physical and logical access controls accomplish the specified restriction.	FISCAM TSD-2.1 CMS Directed NIST 800-26 15.2 NIST 800-26 16.1
Guidance: This can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities.		Related CSRs: 2.3.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Segregation of Duties***

General Requirement / Control Technique	Protocol	Reference
4.6 Employees shall understand their security duties and responsibilities.		
4.6.1 All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	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.	FISCAM TSD-1.3.1 ARS 3.1
Guidance: Employees should have access to their job descriptions and discuss during their performance evaluations.	Related CSRs: 3.1.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	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.	FISCAM TSD-1.3.2 ARS 5.1
Guidance: Senior management is responsible for assuring that employees understand their responsibilities.	Related CSRs: 1.2.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.	1. Review documented procedures identifying responsibilities for restricting access by job position in key operating and programming activities to confirm that these responsibilities are clearly defined. 2. Interview a sample of personnel identified as having the specified responsibilities to confirm that the responsibilities assigned are clearly understood and followed. 3. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-1.3.3
Guidance: A good approach is to develop a matrix identifying resources in relation to organizational access and job title.	Related CSRs: 3.3.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	Review approval controls.	FISCAM TSD-1.1.4
Guidance: Compensating controls should be documented.	Related CSRs:	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. No individual has complete control over incompatible transaction processing functions.	1. Review the required analyses for inclusion of the specified elements. 2. Confirm by review that the required analyses reflect current operations.	FISCAM TSD-1.1.3
Guidance: Establish independent organizational groups with defined functions. Functions and related tasks performed by each unit should be documented.	Related CSRs: 4.1.5	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Segregation of Duties***

General Requirement / Control Technique	Protocol	Reference
4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.	1. Review documentation of process design establishing the specified separation of duties. 2. Confirm through interview, observation, and review of job descriptions for a sample of personnel, that these separation of duties requirements are met. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSD-1.1.5
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.		Related CSRs:
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.7.4 Policies and procedures for segregating duties exist and are up-to-date.	Confirm through inspection that the required policies and procedures exist and are consistent with current operations.	FISCAM TSD-1.1.1
Guidance: Policies are documented, communicated, and enforced.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.7.5 Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Confirm by review that documented operating procedures meet the required criteria.	FISCAM TSD-1.1.6
Guidance: Documentation should be reviewed periodically and updated as needed.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.7.6 Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) quality assurance/testing; (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.	1. Review the agency organization chart showing IS functions and assigned personnel. 2. Interview selected personnel and determine whether functions are appropriately segregated. 3. Review relevant alternative or backup assignments and determine whether the proper segregation of duties is maintained. 4. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.	FISCAM TSD-1.1.2 NIST 800-26 6.1.4 NIST 800-26 17.1.5
Guidance: Manuals and job descriptions include support functions of each individual.		Related CSRs: 3.4.1, 3.4.2, 3.5.4, 3.5.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

5. *Service Continuity*

5.1 Adequate environmental controls shall be implemented.

5.1.1	Building plumbing lines are known and do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known.	1. Examine facility maintenance records for history of water damage. 2. Interview site managers for knowledge of potential pumping related hazards and familiarity with mitigation procedures. 3. Interview a sample of operations staff to confirm familiarity with mitigation procedures for potential plumbing related problems. 4. Observe the operation, location, maintenance, and access to the air cooling systems condensate drains. 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. Review relevant procedures for inclusion mitigation measures for any potential plumbing related problems. 7. Review the current risk assessment to confirm investigation of the potential for plumbing related problems, and review risk mitigation plans for any such risks identified.	FISCAM TSC-2.2.4 ARS 1.9 NIST 800-26 7.1.17

Guidance: The SSO should work in conjunction with the building engineer/maintenance. Related CSRs: 5.6.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.2	Any behavior that may damage computer equipment is prohibited.	1. Review the risk assessment for identification of potentially hazardous employee activities. 2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment. 3. Review job descriptions to ensure there is guidance contained relative to destructive behavior.	FISCAM TSC-2.2.7

Guidance: Management should include behavioral guidance. For example keeping cans of coke on top of a PC could damage it. Related CSRs: 4.3.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.3	Controls have been identified to sufficiently mitigate identified risks and other disasters, such as floods, earthquakes, fire, etc.	1. Review the risk assessment plan for consideration of the specified potential risks. 2. Review documentation of efforts to identify additional risks specific to the region, area, or facility. 3. Review documentation of risk mitigation planning covering all identified risks. 4. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.	FISCAM TSC-2.2.2 ARS 1.9 NIST 800-26 1.2.3 NIST 800-26 7.1.19

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. Related CSRs: 1.8.4, 2.2.14, 5.6.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.1.4 Environmental controls are periodically tested.	1. Review the test plans for future tests. 2. Review test policies. 3. Review documentation supporting recent tests of environmental controls.	FISCAM TSC-2.2.6 ARS 1.9

Guidance: There should be a test plan for the testing of the environmental controls, e.g., humidistat. Related CSRs: 5.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.5 Redundancy exists in the air cooling system.	1. Review facility design documentation confirming air cooling system redundancy. 2. Review maintenance records confirming primary and redundancy systems are operational. 3. Observe demonstrations of operation of primary and redundant cooling systems. 4. Review policy and procedures relevant to operation and maintenance of primary and redundancy air cooling systems	FISCAM TSC-2.2.3 NIST 800-26 7.1.15

Guidance: Only the critical components or subsystems of the entire air cooling system need to be redundant. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.6 Fire suppression and prevention devices have been installed and are working (e.g., smoke detectors, fire extinguishers, and sprinkler systems).	1. Review facility drawings and other documentation documenting types and locations of the specified devices. 2. Review documentation of periodic inspections and maintenance of the specified devices and related systems to assure they are fully operational. 3. Review documentation supporting the qualifications of personnel inspecting and maintaining the specified devices and systems. 4. Observe that fire extinguishers, smoke detectors and sprinkler systems are in place and appear to be in working order.	FISCAM TSC-2.2.1 ARS 1.9 NIST 800-26 7.1.12

Guidance: A good approach is to have the fire department review the systems. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.1.7 An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down.	1. Review facility documentation confirming installation of an uninterruptible power system (UPS). 2. Review design and test data supporting the capacity of the system to support the facility technical load long enough to allow shut down with lose of no more that transactions in progress at the time primary power is lost. 3. Review documentation supporting existence of periodic test, and preventive maintenance consistent with system specifications. 4. Review policies and procedures for orderly shut down of the system within the time allowed by the available UPS capacity. 5. Interview a sample of operations personnel for familiarity with the orderly shut down process and applicable documented procedures. 6. Review documentation supporting periodic test of the orderly shut down process. 7. Observe that secondary power supplies exists.	FISCAM TSC-2.2.5 ARS 1.8 NIST 800-26 7.1.18
Guidance: The facility managers should periodically verify the current computing power load and auxiliary requirements for change.		Related CSRs: 5.9.8, 5.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.1.8 Possible fire ignition sources, such as electronic devices or wiring, storage of combustible materials, and arson possibilities, are reviewed periodically.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review documentation of periodic inspections and storage of combustible materials.	NIST 800-26 7.1.13
Guidance: A good approach is to have the fire department review for possible fire ignition sources.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.1.9 Electric power distribution, heating plants, water, sewage, and other utilities are periodically reviewed for risk of failure.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review documentation supporting recent reviews of environmental controls.	NIST 800-26 7.1.16
Guidance: There should be a process for the testing of the environmental controls and periodic reviews for risk of failure.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2 A Contingency Plan shall be documented in accordance with the CMS Business Partners Systems Security Manual.		
5.2.1 The Contingency Plan provides for backup personnel so that it can be implemented independent of specific individuals.	1. Review the contingency plan to confirm inclusion of the specified provision. 2. Review documentation supporting timely availability of the backup personnel required by the contingency plan. 3. Talk with a random small sample of the designated backup persons to ensure that they understand their role in a contingency.	FISCAM TSC-3.1.2
Guidance: Refer to Appendix B of the BPSSM.		Related CSRs: 5.8.1, 5.10.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement Control Technique	Protocol	Reference
5.2.2 User departments have developed adequate manual processing procedures for use until automated operations are restored.	1. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation. 2. Review the contingency plan for identification of the specified manual procedures. 3. Inspect the required manual procedures for consistency with the contingency plan. 4. Interview the relevant process managers to confirm familiarity with the required procedures. 5. Review test reports to determine that manual procedures have been tested, at least on a sample basis.	FISCAM TSC-3.1.3
Guidance: Determine that the manual procedures have been tested. Refer to Appendix B of the BPSSM.		Related CSRs: 1.8.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.3 The Contingency Plan clearly assigns responsibilities for recovery.	Review the Contingency Plan to confirm clear identification of specific responsibilities for all elements of recovery.	FISCAM TSC-3.1.1 NIST 800-26 9.2.2
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.		Related CSRs: 3.6.4, 4.3.1, 4.6.1, 5.6.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.4 Contingency Plans consist of all components listed in the CMS Business Partners Systems Security Manual, Appendix B, and include detailed instructions for restoring operations.	1. Review Appendix B of the Business Partners Systems Security Manual. 2. Verify through inspection that the Contingency Plan includes the specified elements.	CMS Directed HIPAA 164.310(d)(1) FISCAM TSC-3.1.1 HIPAA 164.308(a)(7)(ii)(C) HIPAA 164.308(a)(7)(ii)(D) HIPAA 164.308(a)(7)(ii)(E) HIPAA 164.308(a)(7)(i) HIPAA 164.308(a)(7)(ii)(A) NIST 800-26 9.2.3 NIST 800-26 12.2.2
Guidance: A business partner Contingency Plan contains the topics described in Appendix B of the Business Partners Systems Security Manual.		Related CSRs: 5.3.1, 5.4.1, 5.4.2, 5.5.1, 5.6.1, 5.8.1, 3.6.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.5 Management, the SSO, and key affected parties approve Contingency Plans.	1. Verify through inspection that all Contingency Plans have been approved by management, SSO, and key affected parties. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-3.1.1 CMS Directed NIST 800-26 9.2.1
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.		Related CSRs: 5.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement / Control Technique	Protocol	Reference
5.2.6 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.	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.	FISCAM TSC-3.1.1 CMS Directed ARS 1.9 ARS 10.8
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.		Related CSRs: 5.5.1, 5.6.1, 5.6.2, 5.6.3, 5.6.4, 5.10.1, 2.6.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.7 The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.	Review the Contingency Plan emergency response procedures for inclusion of the required provision.	CMS Directed HIPAA 164.308(a)(7)(ii)(C) ARS 1.9
Guidance: Ensure that this immediate entry action has been practiced during exercises and training.		Related CSRs: 1.1.7, 2.4.1, 2.4.2, 5.6.1, 5.6.4, 2.2.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.8 Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency plans are re-evaluated before proposed changes are approved.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming that contingency plans have been reevaluated before any proposed major modifications were approved.	CMS Directed
Guidance: Change control management should provide for updates to the Contingency Plan.		Related CSRs: 5.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.9 Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.	1. Review documentation supporting the contention that existing contingency plans protect storage media from improper modification in the event of 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 describing use of software procedures to reduce the potential for data loss and/or modification during a system failure.	CMS Directed NIST 800-26 12.1.9
Guidance: Throughout documentation review and testing, ensure that the safeguards protect data from modification if the system fails.		Related CSRs: 2.5.1, 2.14.2, 3.6.6, 6.4.1, 7.2.2, 9.3.3, 9.8.1, 5.11.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.10 The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.	1. Review test reports. 2. Verify through inspection that the contingency plan identifies the specified interfaces.	CMS Directed
Guidance: Critical interfaces should be tested when the contingency plan is exercised.		Related CSRs: 5.3.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement / Control Technique	Protocol	Reference
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.	1. Verify by inspection that the required, prioritized list has been prepared. 2. Verify by inspection that the list is approved by senior management. 3. Review documentation supporting the contention that the list reflects current conditions. 4. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-1.1 HIPAA 164.308(a)(7)(ii)(E) NIST 800-26 9.1.3
Guidance: It is important to know what critical data and operations are needed to continue critical functions in an emergency.		Related CSRs: 1.9.7, 2.1.3, 5.4.4, 5.8.1, 5.2.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.3.2 There are network diagrams and documentation on setups of routers and switches.	1. Verify by inspection that the required diagrams and setup documentation has been prepared. 2. Review relevant policies and procedures for inclusion of the stated requirements.	NIST 800-26 12.1.4
Guidance: It is important to have network diagrams and documentation on router and switch setups to restore critical functions in an emergency.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.4 Data and program backup procedures shall be implemented.		
5.4.1 System and application documentation are maintained at the off-site storage location.	1. Interview persons at the primary site who are responsible for storing documents off-site. 2. Review documentation supporting maintenance of the required off-site storage. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-2.1.2 NIST 800-26 9.2.7
Guidance: Current systems and applications documentation should be available off-site in case the primary processing site is disabled.		Related CSRs: 5.7.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.4.2 Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent operation of the required rotation. 3. Verify by inspection the location of specific backup files. 4. Review documentation confirming successful periodic test of the ability to recover using backup files.	FISCAM TSC-2.1.1 HIPAA 164.308(a)(7)(ii)(B) NIST 800-26 9.2.6
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.		Related CSRs: 5.11.1, 5.9.8, 5.4.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement Control Technique	Protocol	Reference
5.4.3 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.	1. By inspection, verify that the backup storage and alternate processing sites are consistent with available documentation. 2. Review documentation confirming that the backup storage and alternate processing sites meet the stated requirements.	FISCAM TSC-2.1.3 NIST 800-26 9.2.5 NIST 800-26 9.2.9
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.	Related CSRs: 5.11.2	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.4.4 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.	1. Observe the initiation of delivery of critical data from the primary site to the off-site facility. 2. Review the Contingency Plan to verify that it contains the specified elements. 3. Review records of data backups.	HIPAA 164.310(d)(1) CMS Directed HIPAA 164.308(a)(7)(ii)(A) NIST 800-26 9.1.1
Guidance: Refer to Appendix B of the BPSSM.	Related CSRs: 5.11.1	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.4.5 A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.	An inventory of all equipment and software should be maintained, including the location and person responsible.	HIPAA 164.310(d)(2)(iv)
Guidance: A record should be use to track the movement all resources.	Related CSRs:	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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 logged with name, date, time, and action.	1. Review backup logs. 2. Inspect off-site backups.	ARS 9.9
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.	Related CSRs: 5.4.2	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.	FISCAM TSC-1.3 HIPAA 164.308(a)(7)(ii)(C)
Guidance: Processing priorities should exist for all critical functions and processes to be accomplished during an emergency. These should be periodically reviewed for accuracy.	Related CSRs: 5.3.1, 5.6.4	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Interview a sample of employees to confirm their understanding of their roles in emergency response procedures. 2. Review training records to confirm required training has been conducted, and is consistent with the current procedures. 3. Review training plans for future training in emergency actions.	FISCAM TSC-2.3.1 ARS 4.1 NIST 800-26 9.3.2
Guidance: There should be evidence that the employees have periodically received training relative to what to do in an emergency.	Related CSRs: 1.1.7	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement / Control Technique	Protocol	Reference
5.6.2 Emergency procedures are documented.	By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan.	FISCAM TSC-2.3.3 HIPAA 164.308(a)(7)(i) HIPAA 164.308(a)(7)(ii)(C)
Guidance: Procedures for use in an emergency should exist for automated and manual processes. They should be readily available. Refer to Appendix B of the BPSSM.		Related CSRs: 1.1.7, 2.2.14, 2.4.1, 3.5.6, 4.1.3, 5.2.7, 6.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.6.3 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.	1. Review training records to confirm that the required training has been delivered periodically. 2. Review training plans for future training in emergency actions.	FISCAM TSC-2.3.2
Guidance: These are procedures primarily for staff and management working in a data processing center environment.		Related CSRs: 1.1.7, 5.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.6.4 Emergency procedures are periodically tested.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming completion of the required testing. 3. Review future test plans to ensure that the emergency procedures are scheduled to be properly tested. 4. Interview data center staff.	FISCAM TSC-2.3.4 HIPAA 164.308(a)(7)(ii)(D)
Guidance: 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.		Related CSRs: 5.2.7, 5.5.1, 5.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.7 The contingency plan shall be annually reviewed and tested.		
5.7.1 The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.	1. Review documentation of annual conduct of the required test. 2. Review documentation describing how the testing conditions simulate an emergency or disaster. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review test plans for upcoming contingency plan testing, including lessons learned from the previous testing.	FISCAM TSC-4.1 CMS Directed HIPAA 164.308(a)(7)(ii)(D) ARS 5.4 ARS 5.5 NIST 800-26 4.1.4 NIST 800-26 9.3
Guidance: It is advisable to conduct "live tests" of critical system processes to ensure they will function in an emergency.		Related CSRs: 5.6.4, 2.5.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.7.2 Contingency Plans and associated documentation are reviewed and, if required, updated whenever new operations are planned or new safeguards contemplated.	1. Review the current Contingency Plan to confirm it is updated as required. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-3.1.1 CMS Directed ARS 5.4 ARS 5.5 NIST 800-26 9.2 NIST 800-26 10.2.12
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.		Related CSRs: 1.9.5, 1.12.2, 3.5.6, 6.3.10, 5.2.8
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent annual review, reassessment, and appropriate revision of the contingency plan as specified. 3. Review documentation confirming the required off-site distribution and storage.	FISCAM TSC-3.1.4 FISCAM TSC-3.1.1 FISCAM TSC-3.1.5 CMS Directed NIST 800-26 9.2.10 NIST 800-26 9.3.1

Guidance: Current contingency plans should be readily available to key persons during an emergency. Off-site storage will help ensure this availability. Related CSRs: 5.4.1, 5.9.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.7.4 Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review distribution records or interview senior management to ensure that they received the latest contingency plan test results and lessons learned information.	FISCAM TSC-4.2.1

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. Related CSRs: 3.5.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documents establishing that the contingency plan and related agreements are adjusted as specified.	FISCAM TSC-4.2.2 HIPAA 164.308(a)(7)(ii)(D) NIST 800-26 9.3.3

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.8 Resources supporting critical operations shall be identified.

5.8.1 Resources supporting critical and sensitive operations are identified and documented. Types of 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documents identifying resources supporting critical and sensitive operations for inclusion of the specified resource types.	FISCAM TSC-1.2 NIST 800-26 9.1 NIST 800-26 9.1.2

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. Related CSRs: 5.3.1, 2.1.3, 5.4.4, 5.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.		
5.9.1 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.	1. Interview users. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review the performance records to ensure the goals are clearly stated in writing.	FISCAM TSC-2.4.9
Guidance: To avoid a break in continuity of service, hardware performance should be evaluated frequently and users polled relative to level of service provided.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.2 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of the required logs. 3. Review documentation supporting conduct of the required analyses.	FISCAM TSC-2.4.8
Guidance: Hardware problems should be carefully analyzed in order to determine the maintenance needs and to prevent major failures.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.3 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.	FISCAM TSC-2.4.10
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.		Related CSRs: 1.9.1, 5.7.3, 6.3.4, 10.7.3, 6.6.1, 3.4.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.4 Goals are established by senior management for the availability of data processing and on-line services.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming establishment of the required goals.	FISCAM TSC-2.4.6
Guidance: Reasonable data processing goals should be set by management to guide the maintenance and problem analysis relative to hardware performance and availability.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.5 Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	1. Review records of past advanced notifications. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.	FISCAM TSC-2.4.11
Guidance: Notice of at least 2 days should be given to users relative to hardware changes.		Related CSRs: 5.7.3, 10.7.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement Control Technique	Protocol	Reference
5.9.6 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.	FISCAM TSC-2.4.4

Guidance: The operational flow of business functions should be designed to permit unscheduled interruptions without adversely affecting critical processes and deliveries. Related CSRs: 2.2.24

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.9.7 Records are maintained on the actual hardware performance in meeting service schedules.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the required records.	FISCAM TSC-2.4.7

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. Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.9.8 Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	1. Review documentation confirming availability of spare or backup hardware for support of applications designated as critical or sensitive. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review operations and maintenance documentation to confirm that levels of available backup or spare hardware have been sufficient to support system availability objectives.	FISCAM TSC-2.4.5

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. Related CSRs: 5.4.2, 5.4.3, 5.10.1, 5.11.1, 5.11.2

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.9.9 Hardware maintenance policies and procedures exist and are up-to-date.	1. Inspect maintenance policies and procedures. 2. Review documentation supporting the contention that the required policies and procedures are up-to-date. 3. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	FISCAM TSC-2.4.1

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. Related CSRs: 1.9.1, 1.4.1, 1.8.4

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
5.9.10 Regular and unscheduled hardware maintenance performed is documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance documentation for conformance with the documented procedures.	FISCAM TSC-2.4.3

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.

Related CSRs: 1.8.4, 1.9.5

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.9.11 Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	1. Inspect hardware maintenance schedules 2. Review documentation supporting the contention that the hardware maintenance schedule complies with vendor specifications. 3. Review maintenance records to confirm completion of hardware maintenance in accordance with the schedule. 4. Review documentation supporting the contention that the manner of performing maintenance minimizes the impact of maintenance on operations.	FISCAM TSC-2.4.2 NIST 800-26 7.1.14

Guidance: Maintenance schedules should be distributed and kept at different locations in the enterprise.

Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review documentation supporting the contention that alternate facilities have sufficient processing capacity. 2. Inspect agreements established to confirm coverage of all identified alternate facilities. 3. Review documentation identifying facilities required for alternate data processing and telecommunications. 4. Review documentation supporting the contention that alternate facilities are in the required state of readiness. 5. Review documentation supporting the contention that alternate facilities are available for use.	FISCAM TSC-3.2.1 CMS Directed NIST 800-26 9.2.4

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.

Related CSRs: 2.2.27, 5.1.7, 5.4.2, 5.4.3, 5.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.10.2 Alternate telecommunication services have been arranged.	Review documentation confirming the arrangement of alternate telecommunication services.	FISCAM TSC-3.2.2

Guidance: A careful analysis should be made of all telecommunications utilized in normal times, and the links necessary to support critical functions identified.

Related CSRs: 5.7.5, 5.8.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement / Control Technique	Protocol	Reference
5.10.3 Arrangements are planned for travel and lodging of necessary personnel, if needed.	Verify by inspection that the required arrangements have been planned.	CMS Directed FISCAM TSC-3.2.3

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the required contingency plan(s) to confirm inclusion of the specification of storage location(s) for backup data and software. 2. Review documentation confirming that the specified plan is available for each standalone workstation.	CMS Directed

Guidance: Standalone workstations must be protected and contingency plans made for backup of their resident software and data.

Related CSRs: 5.4.2, 1.13.1, 1.13.5, 2.2.12, 7.4.2, 5.4.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.11.2 Standalone computer workstation backup data, software and current operating procedures are stored in accordance with the Contingency Plan.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Through inspection for a sample of standalone workstations, establish that the specified storage criteria are met.	CMS Directed

Guidance: It is suggested that this back-up information be stored at a location different from the workstations.

Related CSRs: 5.2.9, 5.4.3, 5.4.2, 5.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.12 Detection of malicious software shall be performed.

5.12.1 The CMS Business Partner shall use special software to accomplish malicious software identification, detection, protection, and elimination.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the required software is installed and operational in accordance with documented policy.	FISCAM TCC-1.3.2 HIPAA 164.308(a)(5)(ii)(B)

Guidance: This special software should be approved and tested by knowledgeable persons before being installed.

Related CSRs: 1.1.1, 1.9.1, 2.2.24, 10.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the documented procedure required to process emergency changes. 2. Interview the operations supervisor, computer operations management, programming supervisors, and user management. 3. For a sample of emergency changes, observe the required documentation and approval steps. 4. Review test plans and reports for the emergency changes.	FISCAM TCC-2.2.2 NIST 800-26 10.2.11

Guidance: Ensure that the emergency software changes are subsequently tested.

Related CSRs: 6.3.2, 6.6.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application Software Development and Change Control*

General Requirement Control Technique	Protocol	Reference
6.1.2 Emergency change procedures are documented.	Review the documentation of emergency change procedures.	FISCAM TCC-2.2.1
Guidance: Ensure that the procedures for making emergency software changes are current.	Related CSRs: 1.1.7, 2.4.1, 2.4.2, 3.5.6, 5.6.2, 1.9.3, 10.7.3	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review the required policies, and verify that they are enforced. 2. Interview the security administrator.. 3. Interview users.	FISCAM TCC-1.3.1
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.	Related CSRs: 1.13.2	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3 Changes shall be controlled as programs progress through testing to final approval.		
6.3.1 Test plans are documented and approved that define responsibilities for each party involved.	1. Interview test manager, and others as deemed necessary. 2. Interview the system manager. 3. Verify that test plans are documented and approved, and define the required responsibilities.	FISCAM TCC-2.1.4
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.	Related CSRs: 2.5.11	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.2 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.	1. 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. 2. Review test plan to ensure that it addresses test levels and conditions.	FISCAM TCC-2.1.5
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.	Related CSRs: 2.5.10, 2.5.11, 3.5.1	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.3 A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live test data are not to be used in testing.	1. Confirm the restrictions in the use of live data. 2. Interview test programmers. 3. Interview the system manager. 4. Verify that test data will meet all processing criteria.	FISCAM TCC-2.1.6 FISCAM TCC-2.1.7 ARS 9.8 NIST 800-26 10.2.5
Guidance: 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.	Related CSRs: 1.9.1, 2.5.10, 2.5.11, 3.5.1, 4.7.6, 5.9.3, 6.4.4, 9.8.1	
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application Software Development and Change Control*

General Requirement Control Technique	Protocol	Reference
6.3.4 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.	1. Review documentation of all required departments for prompt and accurate updating. 2. Interview the system manager. 3. Interview the document control person (librarian).	FISCAM TCC-2.1.10 NIST 800-26 3.2.4
Guidance: Documentation used by hardware, software, operations, and systems persons should reflect the latest system and software environment.		Related CSRs: 1.9.1, 1.9.7, 2.5.1, 2.5.10, 3.4.6, 5.4.1, 5.8.1, 6.5.1, 5.9.3, 1.9.3, 10.7.3, 1.2.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.5 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.	1. Interview the software programming supervisor. 2. Review documented software changes to verify the tracing process.	FISCAM TCC-2.1.3
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.		Related CSRs: 2.11.2, 2.11.4, 3.5.6, 6.1.1, 6.6.1, 10.7.3, 6.7.2, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.6 Program changes are controlled as they progress through testing and are moved into production only upon documented approval from users and system development management.	1. Interview user management. 2. Verify the documented approval of program changes before production implementation. 3. Interview system development management.	FISCAM TCC-2.1.9 NIST 800-26 3.2
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.		Related CSRs: 3.4.5, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.7 Test results are reviewed and documented.	1. Verify that test results are reviewed and documented. 2. Interview the system manager.	FISCAM TCC-2.1.8 NIST 800-26 3.2.2
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.		Related CSRs: 2.5.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.8 Changes to detailed system specifications are prepared by the programmer and reviewed by the appropriate supervisor or manager.	1. Interview the programming supervisor. 2. Review documented changes to system specifications.	FISCAM TCC-2.1.2 NIST 800-26 10.2.4
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.9 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).	1. Ensure through observation or interviews that during testing persons/groups fulfilled their responsibilities. 2. Review test plan standards, and confirm that they follow all levels of testing and responsibilities. 3. Interview department supervisors to verify their compliance with test plan standards.	FISCAM TCC-2.1.1
Guidance: A good practice is to have independent tests performed.		Related CSRs: 1.4.4, 2.5.11
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application Software Development and Change Control*

General Requirement Control Technique	Protocol	Reference
6.3.10 Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	1. Interview the system programmers and/or system administrator. 2. Determine when the last production program change was reviewed, and how often. 3. Interview data center management and/or the security administrator.	FISCAM TCC-2.1.11
Guidance: Access controls and change controls should be periodically reviewed and/or tested to ensure their proper function.		Related CSRs: 3.1.2, 3.1.3, 3.3.3, 3.4.1, 4.4.1, 7.3.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.11 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 Roadmap.	1. Interview the system manager. 2. Confirm that the SDLC includes the four required elements.	FISCAM TCC-1.1.1 ARS 3.14 ARS 4.1 NIST 800-26 3.1 NIST 800-26 3.2.1 NIST 800-26 3.1.6
Guidance: Ensure that a current SDLC methodology exists, addresses security has been reviewed, and is being followed.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.12 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.	1. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current. 2. Examine training plans and records. 3. Interview the programming staff and the software staff.	FISCAM TCC-1.1.2 ARS 4.3
Guidance: Training plans and materials should exist for training in SDLC methodology.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.13 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.	1. Interview system programmers and administrators. 2. Interview the application system managers. 3. Review the documented policy to ensure that the required responsibilities are assigned.	CMS Directed HIPAA 164.310(a)(1) ARS 5.1 ARS 10.8
Guidance: Tests should be performed and test reports should be reviewed to ensure that safeguards that protect software from unauthorized modification have been tested.`		Related CSRs: 1.5.2, 1.5.6, 1.9.5, 5.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.14 Immediate (as required functionality allows) installation of vendor-supplied service packs, hotfixes, 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 protect system assets.	1. Review system configuration logs. 2. Review configuration management logs/procedures. 3. Review change approval policies and procedures. 4. Determine if any security fix has not been implemented and time of availability.	ARS 7.17 NIST 800-26 11.1.1
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.		Related CSRs: 1.9.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application Software Development and Change Control*

General Requirement / Control Technique	Protocol	Reference

6.4 Access to program libraries shall be restricted.

6.4.1 Access to all programs, including production code, source code, and extra program copies, is protected by access control software and operating system features.

1. For critical software production programs, determine whether access control software rules are clearly defined.
2. Determine if the access controls are implemented and working.

HIPAA 164.312(e)(1)
FISCAM TCC-3.2.3
HIPAA 164.312(a)(1)

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.

Related CSRs: 5.2.9, 1.4.4, 1.5.6, 2.8.6, 3.3.1, 10.10.1, 2.10.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.4.2 All deposits and withdrawals of program tapes and other storage media to/from the library are authorized and logged.

1. Select other storage media from the log 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 log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tape.

FISCAM TCC-3.2.4
NIST 800-26 7.1.3
NIST 800-26 10.1.2

Guidance: The library log should be protected from exposure to unauthorized changes or release.

Related CSRs: 1.3.12, 2.2.8, 2.2.23, 2.8.6

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.4.3 Production source code is maintained in a separate archive library.

1. Monitor libraries in use.
2. 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.

FISCAM TCC-3.2.2

Guidance: The separate archive library should be protected from unauthorized access by software or physical controls.

Related CSRs: 2.10.2

☑ *SS* ☑ *PSC* ☐ *PartB* ☑ *PartA* ☐ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

6.4.4 Separate libraries are maintained for program development and maintenance, testing, and production programs.

1. Interview library control personnel.
2. Monitor libraries in use.

FISCAM TCC-3.2.1

Guidance: The separate libraries should each have their own set of access controls so that, for example, testers cannot access production code.

Related CSRs: 2.10.2, 3.4.5, 6.8.2, 2.2.29

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.5 Distribution and implementation of new or revised software shall be controlled.

6.5.1 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.

1. Examine distribution and implementation procedures for distributing new or revised software.
2. Check the distribution and implementation orders for a sample of changes.

FISCAM TCC-2.3.2
NIST 800-26 10.2.7
NIST 800-26 10.2.10

Guidance: The implementation order should leave no doubt as to when the new software should start to be used for production.

Related CSRs: 1.9.5, 3.5.1, 6.3.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.5.2 Standardized procedures are used to distribute new software for implementation.

Examine procedures for distributing new software.

FISCAM TCC-2.3.1

Guidance: Software should be distributed allowing enough time at the site for installation, testing, and migration to production.

Related CSRs: 1.9.1, 2.11.2, 3.1.3, 3.4.1, 3.4.4, 3.5.4, 10.7.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Application Software Development and Change Control***

General Requirement Control Technique	Protocol	Reference
6.6 Programs shall be automatically labeled and inventoried.		
6.6.1 Library management software is used to produce audit trails/logs 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.	1. Interview personnel responsible for library control. 2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures. 3. Review software change control policies and procedures.	FISCAM TCC-3.1 ARS 11.2 ARS 11.3 NIST 800-26 10.2.8
Guidance: Software controls should be easily monitored and audited. Library management of software helps ensure that differing versions are not accidentally misidentified.		Related CSRs: 6.3.5, 2.11.2, 2.11.4, 3.5.4, 3.5.6, 5.9.3, 6.1.1, 6.3.5, 10.7.3, 10.10.1, 6.8.2, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.7 Authorizations for software modifications shall be documented and maintained.		
6.7.1 Change requests are approved by both system users and data processing staff.	1. Determine if the change requests for past changes have been approved. 2. Interview software development staff. 3. Identify recent software modifications and determine whether change request forms were used.	FISCAM TCC-1.2.2
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.		Related CSRs: 3.5.4, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.7.2 Software change request forms are used to document software modification requests and related approvals.	Examine a selection of software change or modification request forms for approvals.	FISCAM TCC-1.2.1 NIST 800-26 3.1.4 NIST 800-26 10.2.3
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.		Related CSRs: 3.3.4, 6.3.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.8 Movement of programs and data among libraries shall be controlled.		
6.8.1 Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.	1. Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared. 2. Examine some of the images of stored code that has been changed.	FISCAM TCC-3.3.2
Guidance: An independent library control group should make the image comparisons.		Related CSRs: 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.8.2 A group independent of the user and programmers controls movement of programs and data among libraries.	Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.	FISCAM TCC-3.3.1
Guidance: Prior to moving software from a test to production environment, an independent review of the changes developed and tested should be made.		Related CSRs: 2.10.2, 3.4.2, 6.3.9, 6.4.2, 6.4.4, 6.6.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application System Authorization Controls*

General Requirement / Control Technique	Protocol	Reference

7. *Application System Authorization Controls*

7.1 Source documents shall be controlled and shall require authorizing signatures.

7.1.1 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.

1. Review the documented procedure for batch control sheet preparation.
2. Check a sample of batch control sheets to ensure the inclusion of the Control Technique elements.

FISCAM TAN-1.1.4

Guidance: A preformatted batch control sheet will simplify the tracking process for batch application systems or interactive systems with batching capabilities.

Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

7.1.2 Access to blank documents (checks, claims forms, etc.) is restricted to authorized personnel.

1. Interview a sample of personnel to confirm use of documented handling procedures.
2. Inspect blank document storage access controls for conformance to documented policy.
3. Review documented procedure containing authorized names and control of access.

FISCAM TAN-1.1.1

Guidance: It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents.

Related CSRs: 1.1.8

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

7.1.3 Source documents (checks, claims forms, etc.) are pre-numbered to maintain control over the documents. Key source documents require authorizing signatures.

1. Inspect audit data confirming that the required process is consistently used.
2. Confirm that documents contain authorized signatures.
3. Review the documented procedure for recording and tracking of document numbers.
4. Review documentation identifying "key source documents".

FISCAM TAN-1.1.2
FISCAM TAN-1.1.3

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.

Related CSRs: 2.6.1, 2.13.1

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.

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.

FISCAM TAN-3.1.1

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Application System Authorization Controls***

General Requirement / Control Technique	Protocol	Reference
7.2.2 Master files and program code that does the verification are protected from unauthorized modification.	1. Identify and observe the procedures employed that protect master files and program code. 2. Review the documented procedure covering the protection of master files and program code. 3. Inspect audit data confirming that the required process is consistently used. 4. Review documentation of software controls used in providing the required protection.	FISCAM TAN-3.1.2
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.		Related CSRs: 5.2.9, 2.6.1, 2.13.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3 Data entry workstations shall be secured and restricted to authorized users.		
7.3.1 All transactions are logged as entered, along with the User ID of the person entering the data.	1. Observe the processing of sample transactions, to ascertain that they are being logged correctly. 2. Review the documented procedure prescribing transaction logging.	FISCAM TAN-2.1.9
Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the data entry process is correct.		Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.2 Each operator is required to use a unique password and identification code before being granted access to the system.	1. 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. 2. Review documented login procedure. 3. Observe a sample of data entry login.	FISCAM TAN-2.1.4
Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses, including the use of password and identification control.		Related CSRs: 2.9.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.3 When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	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. Observe physical area during non-business hours.	FISCAM TAN-2.1.2
Guidance: Review the workstation policy/guidelines.		Related CSRs: 1.13.1, 2.2.12
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.4 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.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation use. 3. Observe workstation use.	FISCAM TAN-2.1.5
Guidance: Review the workstation policy/guidelines.		Related CSRs: 1.13.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application System Authorization Controls*

General Requirement / Control Technique	Protocol	Reference
7.3.5 Each workstation automatically disconnects from the system when not used after a specific period of time.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation configuration and use. 3. For a sample of workstation types, observe operation of the automatic disconnect process.	CMS Directed FISCAM TAN-2.1.6 ARS 7.15 ARS 7.16 NIST 800-26 16.2.6
Guidance: Review the workstation policy/guidelines. Additionally, it is a good practice to review the audit logs to validate the workstation disconnect functionality.		Related CSRs: 1.13.1, 2.6.1, 2.13.1, 2.9.11, 2.9.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.6 Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.	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.	FISCAM TAN-2.1.8 NIST 800-26 16.1.1
Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the online access process is correct.		Related CSRs: 6.3.10, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1, 2.9.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.7 Data entry workstations are located in physically secure environments and monitors are positioned to eliminate viewing by unauthorized persons.	1. Review System Security Plan. 2. Observe the location of workstations and their monitors.	FISCAM TAN-2.1.1 NIST 800-26 7.2.1
Guidance: Workstations processing or connected to systems processing sensitive data are located in physically secure areas.		Related CSRs: 2.2.12
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*		
7.4 Users shall be limited to a set of authorized transactions.		
7.4.1 Authorization profiles for users limit what transactions data entry personnel can enter.	1. Review audit controls used to assure continued application of the required procedure. 2. Review documented procedure for data entry to confirm enforcement of the required limitation.	FISCAM TAN-2.2.2
Guidance: Review the application processing policy/guidelines.		Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.4.2 Authorization profiles for users or workstations limit what transactions can be entered.	1. 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. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of configuration management assuring continued operation of the required controls. 4. Review documents designating transactions authorized from each workstation.	FISCAM TAN-2.2.1
Guidance: The supervisors should address limitations in access for inclusion in the ACL.		Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Application System Authorization Controls***

General Requirement Control Technique	Protocol	Reference
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.	1. Inspect audit data confirming that the required process is consistently used. 2. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.	FISCAM TAN-3.2.1
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.		Related CSRs: 1.13.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.6 Independent reviews of data shall occur before entering the application system.		
7.6.1 Procedures are in place for a multilevel review of CMS sensitive input data before it is released for processing.	1. Review documented procedure for pre-processing of data. 2. Interview a sample of supervisors and control unit personnel to confirm use of the process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAN-1.2.3
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.6.2 Data control unit personnel monitor data entry and processing of source documents.	1. Interview management and data control unit personnel to confirm use of the process. 2. Review documented data entry and processing procedures. 3. Observe data entry and processing procedures.	FISCAM TAN-1.2.2
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.		Related CSRs: 8.4.5, 8.5.1, 8.5.2
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
7.6.3 Data control unit personnel verify that source documents are properly prepared and authorized.	1. Inspect audit data confirming that the required process is consistently used. 2. Interview management and data control unit personnel to confirm use of the process. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Observe data control unit personnel performing the verification process.	FISCAM TAN-1.2.1
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.		Related CSRs: 8.4.5, 8.5.1, 8.5.2
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		

Category: *Application System Completeness Controls*

General Requirement / Control Technique	Protocol	Reference

8. *Application System Completeness Controls*

8.1 Computer sequence-checking shall be implemented.

8.1.1	Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review reports of missing or duplicate transactions. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.2.4

Guidance: 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.

Related CSRs: 7.3.1, 7.3.6, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

8.1.2	Sequence checking is used to identify missing or duplicate transactions.	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.	FISCAM TCP-1.2.3

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. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4, 8.2.1

☑ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

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.	1. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers. 2. Review the documented procedure that prescribes the assigning of unique sequence numbers. 3. Inspect audit data confirming that the required process is consistently used. 4. 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. 5. Interview the system owner and determine what policies and corrective action are in place when a sequence number error occurs.	FISCAM TCP-1.2.2

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.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application System Completeness Controls*

General Requirement Control Technique	Protocol	Reference
8.1.4 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.	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.	FISCAM TCP-1.2.1

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.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.	1. Verify the application has an assigned system owner. 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. 4. Verify the application has the ability to insert the preassigned source document numbers matched with the associated data.	FISCAM TCP-1.3.2

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.

Related CSRs: 7.3.1, 7.3.6, 8.1.2, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.	1. Verify that a system owner has been designated and when errors occur, that person is notified. 2. Review the program specifications that describe the computer matching process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.3.1

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.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4, 9.3.5, 9.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the documented procedure that describes the comparison process. 2. Verify that a staff person is assigned and responsible for verifying that high-value transaction data accurately reflects data from the source documentation. 3. Inspect documentation identifying items designated as high-value, low volume. 4. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.4

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.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

Category: ***Application System Completeness Controls***

General Requirement Control Technique	Protocol	Reference
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.	1. Inspect audit data confirming that the required process is consistently used. 2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application. 3. Review the documented procedure describing the reconciliation process.	FISCAM TCP-2.2 NIST 800-26 11.2.1
Guidance: This process is application dependent, but should be automated as much as possible.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review the documented procedures for the data entry process. 2. Review a sample of data control reports for completeness of data entry. 3. This process is application dependent, but should be automated as much as possible. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.	FISCAM TCP-2.1.1
Guidance: The application should be tracking each transaction and reconciling any differences with the data being entered. (commonly called "run-to-run control totals")		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Verify that the application contains routines for process checking. The checking process should be included in applicable trailer labels. 2. Interview the supervisory application programmer to determine that system controls are in place as prescribed by the application programs. 3. Inspect audit data confirming that the required process is consistently used. 4. Review the program specifications describing the reconciliation process for accurate data entry.	FISCAM TCP-2.1.2
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Application System Completeness Controls***

General Requirement / Control Technique	Protocol	Reference
8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	1. Review the documented procedures describing the reconciliation process for data entry. 2. Interview the supervisory application programmer to determine implementation of automatic reconciliation in completion of computer job runs. 3. Inspect audit data confirming that the required process is consistently used. 4. Verify bends and processing errors are reconciled between the completion of one job and before the start of the next job. The reconciliation process should not stop all batch processing.	FISCAM TCP-2.1.3
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
8.4.4 System interfaces require that the sending system's output control counts equal the receiving system's input counts.	1. Review the documented procedure describing the reconciliation process between systems. 2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-2.1.4
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
8.4.5 A data processing control group receives and reviews control total reports and determines the completeness of processing.	1. Review the documented procedure describing the data control group's function. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-2.1.5
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedures for the data control and data entry process for inclusion of the required process.	FISCAM TCP-1.1.2
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		

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.

1. Inspect the process and documents for developing record counts and control totals to determine data entry completeness.
2. Review the documented procedures for the data control process.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM TCP-1.1.1

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.

Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

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 Errors are corrected by the user originating the transaction.

1. Interview a sample of supervisors and subordinate personnel to confirm use of the documented procedure.
2. Inspect audit data confirming that the required process is consistently used.
3. Review the documented error correction procedure.

FISCAM TAY-3.2.2

Guidance: 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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

9.1.2 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.

1. Interview a sample of supervisors and subordinate personnel to confirm that all specified reports and files have the required characteristics..
2. Review sample error reports/files, and confirm that error messages contain the information specified in the Control Techniques.
3. Review the documented error processing procedure.

FISCAM TAY-3.2.1

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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.1.3 All corrections are reviewed and approved by supervisors before the corrections are reentered. (Based on Medicare operating environment CMS Business Partners may have other compensating controls in place.)

1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented error correction procedure for inclusion of the required process.
3. Interview a sample of supervisors and subordinate personnel to confirm use of the required process.

FISCAM TAY-3.2.3

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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference
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.	Review the documentation explaining how the specified objective is met.	FISCAM TAY-1.4

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.

Related CSRs: 2.2.16

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure for processing reject data to confirm inclusion of the specified features.	FISCAM TAY-3.1.1

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.

Related CSRs: 9.1.2, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.1, 9.3.6, 9.7.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.3.2 A control group is responsible for controlling and monitoring rejected transactions.	1. Review the documented procedure describing the control group's responsibilities and duties. 2. Interview a sample of the control group to confirm operational responsibilities match those documented.	FISCAM TAY-3.1.3

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.

Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

9.3.3 General controls effectively protect the suspense file from unauthorized access and modification.	Review the documentation describing how general controls provide the required protection of the suspense file.	FISCAM TAY-3.1.6

Guidance: 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.

Related CSRs: 5.2.9, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

9.3.4 The suspense file is purged of transactions as they are corrected.	1. Review the documented procedure for the error correction process to confirm inclusion of the specified process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-3.1.4

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.

Related CSRs: 2.8.2

☑ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference
9.3.5 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.	1. Review the documented procedure for suspense file processing and transaction reconciliation. 2. Observe the suspense file process to confirm that the documented procedure is followed. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-3.1.2

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.

Related CSRs: 8.2.2

SS	PSC	PartB	PartA	Dmerc	DC	CWF	COB
☑	☑	☑	☑	☑	☐	☑	☑

General Requirement / Control Technique	Protocol	Reference
9.3.6 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.	1. Review the documented suspense file procedure for inclusion of the specified processes. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-3.1.5

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.

Related CSRs: 9.1.2, 9.3.1, 8.2.2, 9.5.1, 9.6.7, 9.6.8, 3.1.5

SS	PSC	PartB	PartA	Dmerc	DC	CWF	COB
☐	☑	☑	☑	☑	☐	☐	☑

9.4 Source documents shall be designed to minimize errors.

General Requirement / Control Technique	Protocol	Reference
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.	1. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry". 2. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.	FISCAM TAY-1.1.1 FISCAM TAY-1.1.2

Guidance: A good approach is to have needed data entry information succinctly formatted to facilitate ease of data entry.

Related CSRs: 1.9.4

SS	PSC	PartB	PartA	Dmerc	DC	CWF	COB
☑	☑	☑	☑	☑	☑	☑	☑

9.5 Overriding or bypassing data validation and editing shall be restricted.

General Requirement / Control Technique	Protocol	Reference
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 logged by the application so that the action can be analyzed for appropriateness and correctness.	1. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-2.3.1 FISCAM TAY-2.3.2

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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

SS	PSC	PartB	PartA	Dmerc	DC	CWF	COB
☑	☑	☑	☑	☑	☑	☐	☑

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference
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.	1. Review the documented procedure assigning responsibility for output production and distribution. 2. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.	FISCAM TAY-4.1.1
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.	Related CSRs: 1.4.4	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming use of the required process. 3. Review documentation describing how the required control is implemented.	FISCAM TAY-4.1.6
Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.	Related CSRs: 9.8.1, 9.8.2	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
9.6.3 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the required schedule to confirm inclusion of the required elements. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-4.1.2
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.	Related CSRs: 1.5.2, 1.5.5	
☐ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
9.6.4 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review sample printed reports to verify that it contains the elements required in the Control Technique.	FISCAM TAY-4.1.3
Guidance: The printed report name, time, and date are good management tools to assist in the tracking of completed tasks.	Related CSRs:	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
9.6.5 Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review logs and check sample output, to verify that the required information is recorded.	FISCAM TAY-4.1.4 NIST 800-26 8.2.3
Guidance: The output report log is a good management tool to assist in the tracking of completed tasks.	Related CSRs: 1.5.2, 3.2.4	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference
9.6.6 Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure describing the output process and supervisory review.	FISCAM TAY-4.1.7

Guidance: The printed reports are good management tools to assist in the tracking of completed tasks. Related CSRs: 1.5.2

☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB

9.6.7 A control log of output product errors is maintained, including the corrective actions taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review the control log and confirm that it contains the required information.	FISCAM TAY-4.1.8

Guidance: The control log, 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. Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB

9.6.8 Output from reruns is subjected to the same quality review as the original output.	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.	FISCAM TAY-4.1.9

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted. Related CSRs: 2.1.2, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB

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.	1. Review the documented procedure describing the review process and detailed report constituency. 2. Inspect audit data confirming that the required process is consistently used. 3. Review sample reports to confirm that they include the required elements specified in the Control Technique.	FISCAM TAY-4.2

Guidance: The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness. Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.4.1, 3.1.5

☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☐ CWF ☑ COB

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.	1. Review the documented procedure describing the protection provided program code, files, or tables. 2. Observe the actions or procedures in place that protect program code, files, or tables.	FISCAM TAY-2.1.4 FISCAM TAY-2.2.1 FISCAM TAY-2.2.2 ARS 9.8

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. Related CSRs: 5.2.9, 9.6.2, 3.4.1

☑ SS ☑ PSC ☐ PartB ☑ PartA ☐ Dmerc ☑ DC ☐ CWF ☑ COB

Category: ***Application System Accuracy Controls***

General Requirement / Control Technique	Protocol	Reference
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.	1. Review the documented procedure describing programmed validation and edits for inclusion of the specifically required checks. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-2.1.1 ARS 9.8
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.		Related CSRs: 9.6.2, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review the documented procedure describing the specified validation and editing process. 2. Inspect audit data confirming that the required process is consistently used. 3. Observe the validation and edit process.	FISCAM TAY-2.1.2 FISCAM TAY-2.1.3 ARS 9.8
Guidance: Validation of the accuracy of data assists in the integrity of the data being processed.		Related CSRs: 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
9.8.4 Integrity verification programs are used by applications to look for evidence of data tampering, errors, and omissions.	Observe the actions or procedures in place that protect Medicare data.	NIST 800-26 11.2.4
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	Observe the actions or procedures in place that protect Medicare data.	NIST 800-26 11.2
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review documented procedure specifying preformatted workstation screens, and describing screen prompts. 2. Observe a sample of workstation screens as personnel are processing data. 3. Interview the system administrator to confirm that the required feature is universally available..	FISCAM TAY-1.2
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement Control Technique	Protocol	Reference

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.

1. By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center.
2. Review audit data confirming control of access lists in accordance with documented procedures.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

Reference: CMS Directed

Guidance: Ensure that only personnel with a need-to-know have access to the list. Related CSRs: 2.2.23

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.1.2 Physical access to enclosures housing network equipment is restricted.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Select a sample of network equipment locations representative of the range of types of physical locations within each facility. For these sample equipment, confirm that access to them is restricted in accordance with the documented procedure.

Reference: CMS Directed

Guidance: Ensure that access to the area where the network equipment is located is controlled. Related CSRs: 2.2.15

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.2 Network system security shall be monitored for deficiencies.

10.2.1 Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation identifying devices selected to provide the specified logging function.
3. By inspection of a sample of the logs, confirm that they include network and system activity.

Reference: CMS Directed

Guidance: Ensure that logs are kept of network activity. Related CSRs: 10.2.4, 2.1.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.2.2 Real-time file scanning is enabled. Desktop virus scanning software is installed, real-time protection and monitoring is enabled, and the software is configured to perform full virus scans during system boot and every 12 hours. Virus-scanning software is provided at critical entry points, such as remote-access servers.

1. Confirm by inspection that virus-scanning software is installed.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation identifying designated critical network entry points.

Reference: CMS Directed
ARS 7.13
NIST 800-26 11.1
NIST 800-26 11.1.2

Guidance: A formal virus protection program should be established at the Network level. Related CSRs: 5.12.1, 10.7.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.2.3 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.	1. Review alarm and alert functions of any firewalls and other network perimeter access control systems to insure they are properly enabled. 2. Review operating system, user accounting, and application software audit logging processes on all host and server systems to insure they are properly enabled. 3. Review relevant policies and procedures for inclusion of the required process. 4. Review sample of intrusion detection audit logs for servers and hosts on the internal, protected, network.	CMS Directed ARS 10.1 NIST 800-26 11.2.5
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.		Related CSRs: 2.6.1, 10.2.5, 10.2.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.4 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.	1. Review network logs. 2. Interview technical staff. 3. Review IDS/Firewall logs. 4. Determine the method for alerts.	ARS 10.2
Guidance: Anomalies should be carefully analyzed to determine if unauthorized activity is occurring. Timely alerts are needed to initiate appropriate activities.		Related CSRs: 10.2.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.5 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 logged. Logs are retained for 90 days, and old logs are archived. Log archives are retained for one year.	1. Review router/firewall configuration. 2. Review router/firewall logs. 3. Determine expiration dates of appropriate logs.	ARS 11.4
Guidance: Ensure that logs from perimeter devices contain the required information, and that they are carefully reviewed on a frequent basis.		Related CSRs: 10.2.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.6 Stateful inspection and application firewall hardware and software are used.	1. Review firewall hardware and software configurations to determine compliance. 2. Utilize firewall reporting capabilities to review log on accounting, active connections, and effectiveness of alert settings.	ARS 6.1 NIST 800-26 16.2.11
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.		Related CSRs: 10.8.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.7 System logs 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.	1. Review alert notifications. 2. Interview technical staff	ARS 10.3 NIST 800-26 11.2.7
Guidance: Establish a policy to review system logs for the required events.		Related CSRs: 10.2.3, 10.9.1, 2.6.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.2.8 If keystroke monitoring is used, users are notified.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-26 17.1.9

Guidance: Establish a policy and procedures on the use and control of keystroke monitoring. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect logs confirming conduct of the required verification.	IRS 1075 5.8@8.2 CMS Directed

Guidance: A good approach might be a policy that requires verification of the receiving facsimile machine's telephone number. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 5.8@8.1 CMS Directed

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." Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.3 Controls exist to identify appropriate use of the E-mail system by employees, and to enforce E-mail authentication, security, privacy, and message integrity.	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-26 11.2.9

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Related CSRs: 10.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.4 Security policy exists and 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the audit process for operation in accordance with the documented process.	CMS Directed ARS 7.4

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. Related CSRs: 10.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.5 Fax procedures 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.	Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 5.8@8.3 CMS Directed

Guidance: Establish a formal procedure generating and attaching the required fax cover sheet. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.6 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 used, they must conform to FIPS 186-2.	Review relevant policies and procedures for inclusion and directed use of the required process.	ARS 8.2 NIST 800-26 15.1.2

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Related CSRs: 10.3.3, 10.3.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement Control Technique	Protocol	Reference

10.4 Cryptographic tools shall be controlled.

10.4.1 Sensitive information being electronically transmitted must be protected. Two acceptable methods for transmitting sensitive information over telecommunications devices: (1) encryption and (2) guided media.

1. Confirm by inspection that documented controls are in place and operational.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation of controls used to assure protection of electronically transmitted sensitive information.
4. Review documentation establishing approval of the protection methods utilized.

HIPAA 164.312(e)(2)(ii)
IRS 1075 5.8@1
FISCAM TAC-3.2.E.1
HIPAA 164.312(a)(2)(iv)
ARS 9.2
NIST 800-26 16.2.14
NIST 800-26 7.2

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.

Related CSRs: 10.4.4, 10.4.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.4.2 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.

1. Review documentation establishing that the required protection has been implemented.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM TAC-3.3
HIPAA 164.312(e)(2)(ii)
HIPAA 164.312(a)(2)(iv)

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.

Related CSRs: 10.4.4, 10.4.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.4.3 The use of application security mechanisms, such as SSL and SSH, is both enabled and forced. Minimum encryption and password authentication are used in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).

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.

ARS 8.1

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Related CSRs: 10.4.1, 10.4.2, 10.5.1, 10.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.4.4 Encryption protection is enabled for wireless media.

1. Review existing policies and procedures to ensure compliant encryption specified.
2. Perform testing to ensure encryption requirement met.

ARS 6.8
NIST 800-26 7.2

Guidance: Data sent via wireless media should be protected using encryption.

Related CSRs: 10.4.1, 10.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.4.5 If encryption is used, it must meet federal standards, and controls for key generation, distribution, storage, use, destruction, and archiving must be implemented.

Review relevant policies and procedures for inclusion and directed use of the required process.

NIST 800-26 16.1.7
NIST 800-26 16.1.8

Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.5 Adequate Network password policies shall be implemented.		
10.5.1 Passwords are transmitted and stored using secure protocols and algorithms.	1. Review documentation of controls used to assure that all systems remain configured to use the specified feature. 2. Review documentation explaining how this feature is implemented on each network and local computing environment. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.7 FISCAM TAC-3.2.E.1 NIST 800-26 15.1.12
Guidance: Ensure that passwords are not transmitted as plain-text.		Related CSRs: 2.9.7, 10.10.1, 10.4.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6 Internet Security Policies shall be made available.		
10.6.1 CMS Business Partner's Internet connections must be in accordance with the CMS Internet Security Policy. 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. (See CMS Internet Security Policy, dated November 24, 1998).	1. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement. 2. 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. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. 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.	CMS Directed ARS 3.8 ARS 9.2 NIST 800-26 16.1.7
Guidance: At present, the internet may not be used for CMS sensitive data.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6.2 Unless prior approval by CMS SSG is obtained, persistent cookies are prohibited.	1. Review software configuration logs/procedures. 2. If not currently in place, procedures to delete cookies should be developed and personnel trained on procedures.	ARS 8.3
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 log files and could also be used to track users browsing habits, cookies just make it easier.		Related CSRs: 1.13.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6.3 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.	Review web pages for compliance.	ARS 3.7 NIST 800-26 16.3.1
Guidance: Privacy policy banners should be displayed on Web pages where personal information is collected.		Related CSRs: 1.7.1, 2.8.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement Control Technique	Protocol	Reference

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.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation describing audit and inventory processes and tools in use to detect improper use of software.

CMS Directed

Guidance: A formal policy should be established regarding the use of purchased software. Related CSRs: 1.13.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.7.2 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.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Confirm by inspection that the specified controls are in place and operating in accordance with the documented procedure.
3. Review documentation describing the software tracking system implemented to provide the specified controls.

CMS Directed

Guidance: A formal program should be established with a policy and procedure. Related CSRs: 1.1.8, 6.5.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.7.3 Change control is implemented to maintain control of changes to hardware, software, and security mechanisms.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming use of the documented change-control mechanism.
3. Review documentation describing the change-control mechanism that is implemented to provide the specified controls..
4. For a sample of hardware, software, and security mechanism, determine by inspection that the configuration of the sample item matches the documented baseline configuration for the item.
5. Compare sampled data, such as device type, serial number, and software version, from the current configuration management baseline system description with corresponding hardware, software, and security mechanism implementation to confirm precise match.

CMS Directed

Guidance: A good approach might be to establish change control policies and procedures for all hardware, software, and security products. Related CSRs: 5.9.3, 6.6.1, 3.4.1, 1.9.3, 6.1.2, 6.3.4, 10.7.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.7.4 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.

1. Review logs.
2. Interview IT personnel.

ARS 10.4

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. Related CSRs: 10.7.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.7.5 All traffic for external communications is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.	Review packet screening rules.	ARS 6.2

Guidance: The packet screening rules should apply only to specified firewalls and routers. Related CSRs: 10.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 a gateway/firewall.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing controls implemented to insure compliance with this requirement.	IRS 1075 5.8@6 CMS Directed FISCAM TAC-3.2.E.1 NIST 800-26 16.2.10

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. Related CSRs: 10.8.5, 10.8.6, 1.13.6, 10.2.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.8.2	Authentication is used 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. Procedures for the above are documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of all required authentication functions.	HIPAA 164.312(d) CMS Directed ARS 1.1 ARS 1.5 ARS 7.1 ARS 7.11 NIST 800-26 16.2

Guidance: A formal program should be established with a policy and procedure. Related CSRs: 2.9.6, 2.9.5, 10.10.2, 10.10.3, 10.4.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review relevant policies and procedures for inclusion and directed use of the required process and specification of the warning message(s) to be used. 2. View the required warning message displayed on the opening screen seen by system users each type of server, workstation, and terminal used in the system. 3. For a sample, including each type of network device supporting the feature, view the required warning message displayed on the opening screen seen by anyone attempting to directly access the device from the network or console.	FISCAM TAC-3.2.E.2.1 ARS 3.6 NIST 800-26 16.2.13

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. Related CSRs: 2.8.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.8.4	Workstations with dial-up access generate a unique identifier code before connection is completed.	1. Review documented dial-up procedure to confirm inclusion of the required features. 2. Observe a sample of dial-up connections involving each type of access controller.	FISCAM TAN-2.1.7

Guidance: If workstations have dial-up access, ensure that a unique ID code is generated for each dial-up session. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.8.5 All servers allowing public access are placed within a DMZ, and direct access is not allowed to the internal network. DMZ servers cannot access the internal network. DMZ packet filtering and proxy rules provide protection for servers.	1. Review network diagrams for proper configuration in relation to 'CMS Internet Architecture document number CMS-CIO-STD-INT01'. 2. Review packet filtering/proxy rules.	ARS 6.6
Guidance: The architecture and the use of rules should prohibit unauthorized access to all servers.		Related CSRs: 10.8.1
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.8.6 All network protocols not explicitly required for system and application functionality are disabled.	1. Examine network configuration logs for compliance. 2. Randomly review network protocols on desktop systems. 3. Review the policy/procedure.	ARS 7.10 NIST 800-26 16.2.2
Guidance: Develop and implement a way to verify that the protocols that are not required have been disabled.		Related CSRs: 2.3.1, 10.8.1
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.9 Vulnerabilities to physical and cyber attacks shall be assessed.		
10.9.1 A plan is in place to assess the risks to the network.	Review the required plan and approved implementing instructions.	PDD 63 333
Guidance: A formal program is in place for determining when and how to assess risks to the network.		Related CSRs: 10.2.7
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.9.2 A plan is developed for eliminating significant vulnerabilities.	1. Review the required plan. 2. Review documentation establishing that the required plan eliminates all significant vulnerabilities.	PDD 63 338 NIST 800-26 10.3
Guidance: As part of the security management program, ensure that a plan is developed to minimize vulnerabilities.		Related CSRs:
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.9.3 A plan is developed for alerting, containing, and rebuffing a physical or cyber attack on the CMS Business Partner IS systems.	Review the required plan to confirm that it includes the specified features.	PDD 63 350
Guidance: A formal program should be established with documented policies and procedures.		Related CSRs:
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.9.4 Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming conduct of the required assessments at least annually.	PDD 63 333 ARS 1.2
Guidance: As part of the security management program, ensure that an annual assessment is performed.		Related CSRs: 1.9.8, 10.9.5
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.9.5 Penetration testing is performed as needed, and 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.	1. Review IOM summarizing the results of the penetration testing. 2. Interview SSO to determine findings and relevant documents.	ARS 10.7 NIST 800-26 1.1.5 NIST 800-26 2.1.4 NIST 800-26 10.3.1 NIST 800-26 10.3.2 NIST 800-26 11.2.8
Guidance: There should be documentation available showing that the penetration testing was accomplished according to appropriate standards and procedures.		Related CSRs: 10.9.4
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.9.6 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.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-26 14.2 NIST 800-26 14.2.1 NIST 800-26 14.2.2 NIST 800-26 14.2.3

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 IDs 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 logs; (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.	1. Review documentation confirming implementation of communications software having all of the required features. 2. Review audit data confirming continuing operation of all specified features of the required software.	FISCAM TAC-3.2.E.1 ARS 7.15 ARS 7.21 NIST 800-26 7.2.2 NIST 800-26 16.2.1 NIST 800-26 16.2.8 NIST 800-26 16.2.9 NIST 800-26 16.2.15

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.

Related CSRs: 6.4.1, 2.9.6, 2.9.11, 2.8.4, 3.4.1, 2.9.8, 2.9.10, 3.6.2, 10.5.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.10.2	Remote access is enabled through VPN links, using authorized VPN client software. Encryption standards are used in combination with password authentication and certificate-based authentication or additional authentication protection (e.g., token-based, biometric).	1. Review remote access policies/procedures. 2. Check that remote access is implemented and controlled.	ARS 7.19

Guidance: Remote access should be controlled and there should be evidence of that control.

Related CSRs: 3.6.3, 10.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.10.3	Secure management protocols are enabled through VPN link(s) if connected to a network, and Remote Administration is used. Encryption standards are used in combination with password authentication or additional authentication protection (e.g., token-based, biometric).	☐Review remote access policies/procedures.	ARS 7.20

Guidance: Remote administration should be carefully managed and controlled. Use of encryption features should be evaluated and approved by knowledgeable persons.

Related CSRs: 2.9.5, 10.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference

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).	1. Review training syllabus for inclusion of the required training. 2. Review a sample of training records to confirm completion of the required training. 3. Review documented procedure for generation of security reminders. 4. Review the training policy. 5. Interview a sample of site personnel to verify that documented training was received.	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) FISCAM TSP-4.2.2 PDD 63 358 ARS 4.1 ARS 4.3 NIST 800-26 13.1.4

Guidance: A formal program should be established with a policy and a procedure. Related CSRs: 5.12.1, 2.9.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.1.2	Security skill needs are accurately identified and included in job descriptions.	1. Review a sample of job descriptions for identification of security skills required. 2. Evaluate the apparent relevance of the specified security skills to the job described.	FISCAM TSP-4.2.1

Guidance: The SSO should work in conjunction with the HR department on job description updates. Related CSRs: 3.3.3, 3.6.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.1.3	All personnel (employees and contractors) are provided security awareness and security training prior to being allowed access to CMS sensitive information or data, and security awareness is repeated, minimally, on an annual basis.	1. Review training syllabus for inclusion of security awareness training. 2. Review policies and procedures for inclusion of the required process. 3. For a sample of personnel having access to sensitive information, review personnel records for documentation of receipt of security awareness training. 4. For a sample of personnel having access to sensitive information, review training documentation and job descriptions for apparent customization of security awareness training to job responsibilities. 5. Interview a sample of personnel having access to sensitive information to determine if they are aware of their responsibilities relating to handling of sensitive information. 6. Verify that records show training occurred prior to access to sensitive data.	FISCAM TSP-3.3.1 IRS 1075 6.2@1 CMS Directed PDD 63 358 HIPAA 164.308(a)(5)(i) ARS 4.4 NIST 800-26 13.1.3

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.1.4 Security training 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).	For a sample of personnel, review training documentation and job descriptions for evidence of customization of security training to the level of job responsibilities.	CMS Directed NIST 800-26 13.1
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).		Related CSRs: 3.2.1, 3.2.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.5 The employees acknowledge, in writing, having received the security and awareness training.	1. Verify that records show all employees have acknowledged receiving security and awareness training. 2. Check a random sample of employees records to verify training attendance signature.	FISCAM TSP-4.2.3 CMS Directed ARS 4.1 ARS 4.3 NIST 800-26 13.1.2
Guidance: No further guidance required.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.6 A record of the security awareness and security training subject(s) covered is maintained.	Verify that records are being maintained that document the security awareness and security training subjects covered.	CMS Directed
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.7 Training in emergency procedures is conducted at least once a year.	Verify the emergency procedures are dealt with in the COOP.	CMS Directed NIST 800-26 12.1.8
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.		Related CSRs: 5.6.1, 5.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.8 Policy and security training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided.	Review documentation of policy and training to confirm the protection of copyright information under the terms of the provision of the copyright holder.	CMS Directed
Guidance: A security policy should exist, and security training should include, appropriate information regarding copyright protection.		Related CSRs: 3.3.1, 7.1.2, 10.7.2, 2.2.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.9 When individuals are authorized to bypass significant technical and operational controls, or when controls cannot adequately protect the information, the affected individuals are screened prior to access and periodically thereafter.	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.	NIST 800-26 6.2.1 NIST 800-26 6.2.3
Guidance: Screening should be consistent with the criteria established for the sensitivity designation of the assigned position.		Related CSRs: 1.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.1.10 A help desk or user support group is available to offer advice.	Interview a sampling of users to determine if a help desk or support group is available to offer advice.	NIST 800-26 8.1 NIST 800-26 8.1.1
Guidance: Possible implementations of incident support resources include a help desk or support group.		Related CSRs: 2.9.18
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference

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.

1. Records providing information on the monitoring activities should be available.
2. Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested.
3. Review logs and policy documentation to verify that security corrective actions have been monitored on a continuing basis.

Reference: FISCAM TSP-5.2; HIPAA 164.316(b)(2)(iii)

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.

Related CSRs: 1.8.7, 1.12.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.2.2 There is an effective and timely process for reporting significant weaknesses and ensuring effective remedial action.

1. Review audit and review findings for their inclusion in the POA&M.
2. Review relevant policies and procedures for inclusion of the required process.

Reference: NIST 800-26 2.2.1

Guidance: The Plan of Action and Milestones (POA&M) updates are based on the findings from security control assessments, security impact analysis, and continuous monitoring activities.

Related CSRs: 2.1.1, 2.13.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.2.3 Budget requests (e.g., Line One funding, safeguards) include the security resources required for the system.

1. Review relevant policies and procedures for inclusion of the required process.
2. Review budget requests for inclusion of security resources necessary for the system.

Reference: NIST 800-26 3.1.5

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.

Related CSRs: 4.6.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.2.4 Security controls are consistent with, and an integral part of, the IT architecture of the business partner.

Review relevant policies and procedures for inclusion of the required process.

Reference: NIST 800-26 3.1.9

Guidance: The information system-required documentation includes security configuration settings and security implementation guidance. They should also provide the required security capabilities and required design and development processes.

Related CSRs: 6.3.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference

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.)

1. Review disclosure list for entries indicating that the documented process has been followed.
2. Interview responsible individual(s) to confirm understanding of the required procedure.
3. Review relevant policies and procedures for inclusion of the required logging process elements.
4. For a sample of documents being received from the IRS, observe handling of receipt of sensitive information for compliance with established procedures.

IRS 1075 3.3@2.2

Guidance: Transmission of Federal Tax Information must be accompanied by appropriate records that will determine who released the information and what was released.

Related CSRs:

☐ ***SS*** ☐ ***PSC*** ☐ ***PartB*** ☐ ***PartA*** ☐ ***Dmerc*** ☐ ***DC*** ☐ ***CWF*** ☑ ***COB***

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.

1. Observe transmittal of sensitive information for compliance with established procedures.
2. Review relevant policies and procedures for inclusion of the required logging process elements.
3. Review disclosure list for entries indicating that the documented process has been followed.
4. Interview responsible individual(s) to confirm understanding of the required procedure.

HIPAA 164.312(c)(2)
HIPAA 164.312(e)(2)(I)
IRS 1075 3.3@2.1
HIPAA 164.312(c)(1)
ARS 11.6

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.

Related CSRs: 2.12.2

☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***

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 for the logging of shipping and receipts and a periodic reconciliation of these records.

1. Evaluate the identified control procedures for inclusions of maintenance of records logging all shipping and receipts, and of periodic reconciliation of these records.
2. Review documented procedures for control of sensitive data entering or leaving the facility.
3. Evaluate the identified control procedures for inclusions of specific protections against erroneous or unauthorized transfers.
4. Review policy for relevance.

CMS Directed
HIPAA 164.310(d)(2)(iii)
NIST 800-26 8.2.2

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.

Related CSRs: 2.2.25, 2.2.26

☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.3.4 A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.	1. Review the documented procedure for destruction of data. 2. Verify that the reviewed procedure includes protections against sensitive data becoming available to unauthorized personnel.	CMS Directed ARS 1.6
Guidance: A good concept is to establish a formal program with a policy and procedures for developing and maintaining records. A record should be maintained that verifies who performed the destruction and when sensitive information was destroyed.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.3.5 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. Ensure the destruction of any sensitive information hard copy documents when no longer needed.	1. Review disposal procedures for inclusion of use of approved destruction methods during disposal of hard copy documents that are no longer needed. 2. For a sample of employees, interview to determine that disposal procedures are known and being followed. 3. Review disposal procedures for inclusion of use of approved sanitization procedures before release of any nonvolatile storage devices or media. 4. Review disposal procedures for inclusion of protections against use of retired, discarded, or unneeded sensitive data by unauthorized persons.	HIPAA 164.312(c)(2) IRS 1075 6.3@6 HIPAA 164.312(e)(2)(i) CMS Directed HIPAA 164.310(d)(2)(i) HIPAA 164.310(d)(2)(ii) HIPAA 164.312(c)(1) ARS 9.6 NIST 800-26 3.2.11 NIST 800-26 8.2.8 NIST 800-26 10.1.3
Guidance: A good approach assures policies and procedures exist for release and/or destruction of CMS sensitive information.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.3.6 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]).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. By inspection confirm that the specified data and records are stored on-site.	CMS Directed
Guidance: When utilizing commercial storage facilities for off-site storage, ensure that any agreements in place address these Federal standards.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.3.7 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review a sample of destruction records to confirm consistent use of the procedure.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.308(a)(4)(i) HIPAA 164.310(d)(2)(ii) HIPAA 164.310(d)(2)(iii) IRS 1075 8.4@1 HIPAA 164.312(c)(1) ARS 9.5
Guidance: A formal program should be established with a policy and procedure. Review and update existing policy and procedures for addressing these requirements.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.3.8 Before releasing files containing sensitive information to an individual or contractor not authorized to access sensitive information, care is taken to remove all such sensitive information. 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 log is used to document that all discarded or transferred items are examined for sensitive information and this information is cleared before the items are released.	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.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(d)(2)(i) HIPAA 164.310(d)(2)(ii) IRS 1075 5.3@2.3 FISCAM TAC-3.4 HIPAA 164.312(c)(1) ARS 1.6 ARS 9.5 NIST 800-26 3.2.12 NIST 800-26 3.2.13 NIST 800-26 8.2.9

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.

Related CSRs: 2.12.2, 2.14.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.9 FTI is physically destroyed by authorized personnel, or returned to the originator or to the system security administrator. (This CSR applies only to the COB contractor.)	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.	IRS 1075 6.3@6

Guidance: A formal security program should be established with a policy and procedure.

Related CSRs:

☐ *SS* ☐ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

1.3.10 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. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)	1. Confirm by inspection that facility has latest version of IRS Publication 1075. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming consistent use of the required receipt process.	IRS 1075 8.1

Guidance: It is a good approach when returning FTI information to CMS 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.

Related CSRs:

☐ *SS* ☐ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

1.3.11 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.	1. Review documentation confirming that destruction is accomplished using one or more of the approved methods. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) IRS 1075 8.3 HIPAA 164.312(c)(1) ARS 9.6 NIST 800-26 8.2.10

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.3.12 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 recorded in a log 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 log 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 logged.	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.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(d)(2)(iii) IRS 1075 4.6@3 HIPAA 164.312(c)(1) FISCAM TAC-3.1.A.6 CMS Directed IRS 1075 3.2@1.3 IRS 1075 3.2@2.2 PDD 63 193 ARS 1.6 NIST 800-26 8.2 NIST 800-26 8.2.7 NIST 800-26 10.2.9

Guidance: One method would be to ensure that deposits and withdrawals of tapes and other storage media from the library are authorized and logged and that audit trails kept as part of inventory management.

Related CSRs: 1.5.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.13 Semiannual inventories of removable storage devices and media containing sensitive information are performed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.	IRS 1075 3.2@2.3 PDD 63 193

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.14 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.	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.	IRS 1075 3.2@1.1 PDD 63 193

Guidance: A formal program should be established with a policy and procedure.

Related CSRs: 2.2.31

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.3.15 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. Media holding, processing or storing sensitive data is kept in a secure area.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming location of computer operations are in a secure area with restricted access, or that establishes approved use of equivalent safeguards.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(a)(1) HIPAA 164.310(c) IRS 1075 4.6@1.2 IRS 1075 4.6@1.5 HIPAA 164.312(c)(1) PDD 63 193 CMS Directed ARS 9.3 ARS 9.4 ARS 9.7 NIST 800-26 8.2 NIST 800-26 8.2.7 NIST 800-26 10.2.9

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).

Related CSRs: 2.2.16, 2.5.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
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.	1. Review a sample of training records to confirm completion of security awareness training. 2. Review training syllabus for inclusion of the security awareness training. 3. Review relevant policies and procedures for inclusion of the prescribed features. 4. Review personnel security records and job descriptions to verify that operating and maintenance personnel have the proper clearances. 5. Review access and maintenance logs, and interview a sample of operating and maintenance personnel, to verify that all maintenance access is logged, and that all maintenance is performed or supervised by authorized, knowledgeable personnel. 6. Review the process for requesting, establishing, issuing, and closing user accounts.	HIPAA 164.308(a)(3)(i) HIPAA 164.308(a)(3)(ii)(A) HIPAA 164.308(a)(3)(ii)(B) ARS 1.5 ARS 1.6 ARS 1.7 ARS 3.13 ARS 4.1 ARS 4.3 NIST 800-26 6.1.8 NIST 800-26 10.1 NIST 800-26 10.1.1 NIST 800-26 10.1.3
Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information.		Related CSRs: 4.2.2, 1.8.4, 2.2.19, 3.5.2, 5.9.9, 2.8.3, 2.8.5, 2.8.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.2 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.	1. Review relevant policies and procedures for inclusion of the required self assessment process. 2. Review documentation confirming submittal of the most recent self assessment to CMS.	HIPAA 164.316(b)(2)(iii) IRS 1075 6.3@1 HIPAA 164.308(a)(8) NIST 800-26 2.1.3
Guidance: Annually complete the self assessment utilizing the Contractor Assessment Security Tool (CAST), and run the "Error Check Self-Assessments."		Related CSRs: 2.12.1, 1.8.6, 2.5.7, 2.5.8, 2.5.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.3 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.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm familiarity with the policy and how to report such improper activity.	IRS 1075 10.1 HIPAA 164.308(a)(6)(ii) FISCAM TAC-4.3.3
Guidance: Establish procedures to identify apparent security violations and ensure that suspicious activity is investigated and appropriate action taken.		Related CSRs: 1.4.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.4 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.	1. Review policies and procedures for the required distribution process(es). 2. Review the distributed security policies for inclusion of the required rules. 3. Interview a sample of site personnel to verify that security policies are distributed.	FISCAM TSP-3.3.2 HIPAA 164.308(a)(1)(i) NIST 800-26 4.1.3 NIST 800-26 13.1.1 NIST 800-26 13.1.5
Guidance: Establish procedures to distribute the security policies to all necessary personnel, and develop a process to document the receipt by the personnel.		Related CSRs: 6.4.1, 6.3.9, 9.6.1, 1.5.1, 1.9.11
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.4.5 Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. 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.	Review relevant policies and procedures for inclusion and directed use of the required procedures.	CMS Directed HIPAA 164.308(a)(6)(i) HIPAA 164.308(a)(6)(ii) ARS 10.5
Guidance: A good approach is to access the CERT WEB site for sample procedures for inclusion. Related CSRs: 1.6.3, 1.4.3		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.6 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.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm awareness of, and adherence to this policy.	CMS Directed
Guidance: Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business. Related CSRs: 2.9.13		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.4.7 Employees are made aware that company policy prohibits the browsing of sensitive data files for any reason other than Medicare business.	1. Interview a sample of employees to confirm awareness of, and adherence to this policy. 2. Review relevant policies for inclusion of the required directive.	CMS Directed
Guidance: Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business. The employee should have a valid need-to-know. Related CSRs:		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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 responsibilities and expected behaviors 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.	1. 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. 2. 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.	FISCAM TSP-3.2 ARS 3.1
Guidance: Ensure that the Rules of Behavior are contained in the SSP and that they clearly define the responsibility of all employees. Related CSRs: 1.4.4		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	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.	FISCAM TSP-3.1.2 CMS Directed HIPAA 164.308(a)(2) ARS 4.6 NIST 800-26 4.1.6
Guidance: An approach is to certify or ascertain that the SSO has a CISA, CISSP or other appropriate information security certification. Related CSRs: 9.6.3, 9.6.5, 9.6.6		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.5.3 If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.	1. If these additional SSO positions exist, review documentation supporting use of the specified process. 2. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed ARS 4.6
Guidance: Ensure that all Medicare related actions are cleared through the primary Medicare SSO. Related CSRs:		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.4 The SSO is organizationally independent of IS operations.	Review documentation supporting the required organizational independence.	CMS Directed
Guidance: Ensure that the SSO's duties allow him/her to act independent of IS operations. Related CSRs: 1.9.10		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.5 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.	1. Review documentation supporting SSO performance of each of the specified roles and responsibilities. 2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.	HIPAA 164.316(b)(2)(iii) CMS Directed
Guidance: An approach is to include these in the SSO's job description. Related CSRs: 9.6.3, 3.1.2, 1.9.4		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.6 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.	1. Review relevant documentation for designation of this security officer. 2. Review relevant policies and procedures for inclusion of identification of the specified roles and responsibilities of this security officer.	CMS Directed ARS 10.8
Guidance: An approach is to include these in the SSO's job description. Related CSRs: 6.3.13		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.5.7 Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.	Review documentation supporting designation of this responsibility to specific employees.	IRS 1075 3.2@1.2 FISCAM TAC-3.1.A.3 HIPAA 164.308(a)(2) HIPAA 164.310(d)(1)
Guidance: A good approach is to have the SSO designate specific employees this responsibility. Related CSRs: 1.3.12, 2.2.31		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.5.8 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.	1. Review documentation supporting SSO performance of each of the specified roles and responsibilities. 2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities. 3. Review contracts, RFPs, and other solicitation documentation for inclusion of the specified requirements.	ARS 3.3 NIST 800-26 3.1.10 NIST 800-26 3.1.11 NIST 800-26 3.1.12 HIPAA 164.308(b)(1) HIPAA 164.308(b)(4) HIPAA 164.314(a)(1)
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.		Related CSRs: 1.11.2
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

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.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Review security incident procedures	HIPAA 164.308(a)(1)(ii)(D) HIPAA 164.308(a)(6)(i) ARS 4.8 ARS 10.5 NIST 800-26 14.1.6
Guidance: Refer to sample procedures from the CERT website.		Related CSRs: 1.6.3
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
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 means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; (5) links to other relevant groups; and (6) receipt and response to other pertinent security alerts/advisories.	Review documentation supporting existence of the required characteristics within the Business Partner's incident response capability.	FISCAM TSP-3.4 ARS 1.9 ARS 4.8 ARS 10.5 NIST 800-26 2.1.5 NIST 800-26 14.1 NIST 800-26 14.1.1 NIST 800-26 14.1.2 NIST 800-26 14.1.3 NIST 800-26 14.1.4 NIST 800-26 14.1.5
Guidance: Refer to sample procedures from the CERT WEB site.		Related CSRs: 1.6.3
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
1.6.3 Relevant security incident information is documented according to 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.	1. Review Incident Handling procedures. 2. Interview response team personnel. 3. Examine secure storage area.	ARS 10.6
Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.		Related CSRs: 1.6.2, 1.4.5, 1.6.1, 1.9.3
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

1.7 Sensitive data to be protected shall be divided into Security levels as appropriate.

1.7.1 CMS has categorized sensitive Medicare data, FTI, and Privacy Act-protected data as sensitive information. These items are to be protected under the CMS Level 3 - High Sensitive security designation.	Sensitive Information Safeguard Requirements verify that the combinations of protection implemented for Level 3 sensitive data match those specified in the Business Partners Systems Security Manual, Section 4.1.1.3.	FISCAM TAC-1.1 IRS 1075 4.1@2 CMS Directed
Guidance: Ensure that a policy and procedure exist to categorize and protect all Medicare sensitive data as level 3 (See BPSSM).		Related CSRs: 2.5.2, 2.7.1, 2.2.7, 10.6.3
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
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.	Review relevant policies and procedures for inclusion of the required security management features.	HIPAA 164.308(a)(1)(ii)(A) HIPAA 164.308(a)(1)(ii)(B) HIPAA 164.308(a)(1)(ii)(C) ARS 3.1 ARS 3.6
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.		Related CSRs: 3.1.2, 1.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.8.2 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.)	Confirm by inspection that the required documentation and agreements is on file.	FISCAM TSP-1.3 HIPAA 164.308(a)(1)(ii)(A) NIST 800-26 1.2.1 NIST 800-26 3.1.8
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.		Related CSRs: 3.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.8.3 The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	1. Review risk assessment policy for inclusion of the required factors. 2. Review the most recent high-level risk assessment for documentation of consideration of the required factors.	FISCAM TSP-1.2 HIPAA 164.308(a)(1)(ii)(A) ARS 3.2 NIST 800-26 1.1.3 NIST 800-26 4.1.7
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.		Related CSRs: 3.1.2, 2.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.8.4 A 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 trails/logs, 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).	1. Review relevant policies and procedures for inclusion and directed use of the required process for determining the need for reassessment. 2. Review relevant policies and procedures for inclusion and directed use of the required content. 3. Review the most recent risk assessment for documented inclusion of the required content.	CMS Directed FISCAM TSP-5.1.1 HIPAA 164.308(a)(1)(ii)(A) FISCAM TSP-1.1 PDD 63 165 ARS 5.3 ARS 9.5 ARS 10.8 NIST 800-26 1.1.2 NIST 800-26 3.1.7 NIST 800-26 4.1.1 NIST 800-26 4.1.2
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.		Related CSRs: 3.1.2, 3.1.3, 1.4.1, 2.2.19, 3.5.2, 5.9.9, 1.12.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.8.5 Facilities housing sensitive and critical resources have been identified. 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. Adequate physical security controls have been implemented that are commensurate with the risks of physical damage or access.	1. Review documentation supporting an assessment that all facilities housing sensitive and critical resources have been identified. 2. 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.	FISCAM TAC-3.1.A.1 FISCAM TAC-3.1.A.2 ARS 1.1 ARS 1.3 NIST 800-26 1.1.4 NIST 800-26 7.1
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.		Related CSRs: 1.9.3, 1.9.8
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.8.6 A compliance review and self-assessment is conducted once a year.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming execution of the review process at least once a year.	CMS Directed

Guidance: Ensure that the CAST is completed once a year and that it is independently verified. Related CSRs: 1.4.2, 2.5.7, 2.5.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.7 Top management initiates prompt actions to correct deficiencies and ensures that corrective actions are effectively implemented.	1. Review documentation supporting consistent prompt action by top management to correct deficiencies. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSP-5.1.4 NIST 800-26 2.2 NIST 800-26 4.2.1

Guidance: An approach is to have senior management approve the corrective action plan and have quarterly updates to the plan. Related CSRs: 1.2.1, 1.12.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.8 Major systems and applications are approved by the managers whose missions they support.	1. Inspect documentation of approval for each major system and application by the specified manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSP-5.1.3

Guidance: Refer to the CMS SSPM for additional information guidance. Related CSRs: 1.9.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.9 Local Information System risk factors are periodically assessed in accordance with the CMS Information Security Risk Assessment (RA) Methodology and NIST SP 800-30.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying assessment of local risk factors in accordance with the reference.	CMS Directed ARS 5.2 NIST 800-26 1.1 NIST 800-26 12.2.4

Guidance: This CSR should be addressed as part of a formal Risk Management Program. Related CSRs: 1.9.8, 1.9.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.8.10 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 CMS Level 3 - High Sensitivity security designation.	Review documentation establishing that a location-specific Risk Analysis was conducted in development of each applicable System Security Plan.	CMS Directed IRS 1075 4.2 ARS 3.2

Guidance: See the Business Partners Security Manual for additional information and guidance. Related CSRs: 2.2.11, 2.2.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.9 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.

1.9.1 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.	1. Review the security plan for inclusion of the required elements. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation supporting completion of the required security testing. 4. Review system configuration documentation for inclusion of links to other systems.	HIPAA 164.308(a)(5)(ii)(B) HIPAA 164.310(a)(2)(iv) ARS 3.4 ARS 3.13 NIST 800-26 1.1.1

Guidance: Policies and Procedures should exist that address these control objectives. Related CSRs: 5.9.3, 5.12.1, 2.5.1, 6.3.14

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.9.2 Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.	Review relevant policies and procedures for inclusion and directed use of the required process.	HIPAA 164.308(a)(1)(ii)(A) ARS 3.13
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.11.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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) personnel controls/personnel security; (d) incident response capability; (e) continuity of support/contingency planning; (f) technical security/technical controls; (g) system interconnection/information sharing; (h) public access controls.	1. Review documentation verifying that a security plan covers all major facilities and operations. 2. Review documentation verifying that the security plan has been approved by all key affected parties. 3. Inspect the security plan to confirm that it covers all of the specified topics.	FISCAM TSP-2.1 HIPAA 164.310(a)(1) HIPAA 164.310(a)(2(ii) HIPAA 164.310(a)(2(i) HIPAA 164.308(a)(4)(i) ARS 3.13 ARS 4.7 ARS 4.8
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.8.8, 6.1.2, 6.3.4, 10.7.3, 2.10.6, 1.6.3, 1.8.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.4 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).	1. Review documentation establishing that preparation of the plan was in accordance with the CMS SSP Methodology. 2. Review documentation verifying coverage by system security plans for all applications categorized as MA and GSS. 3. Review SSP to determine if approval signatures are included	CMS Directed ARS 1.9 ARS 3.13 ARS 5.6 NIST 800-26 3.2.8 NIST 800-26 4.1.5 NIST 800-26 5.1 NIST 800-26 5.1.2 NIST 800-26 12.2.1
Guidance: Refer to the CMS System Security Plans Methodology for further guidance.		Related CSRs: 9.4.1, 3.2.4, 3.3.2, 3.4.6, 3.5.2, 3.5.3, 3.5.6, 3.6.2, 3.6.3, 1.8.1, 1.5.5, 1.12.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.5 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 trails/logs and visitor sign-in sheets. Include all other CMS directed or Business Partners System Security Manual directed documents.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.	HIPAA 164.316(b)(1) HIPAA 164.316(b)(2)(ii) HIPAA 164.316(b)(2)(iii) CMS Directed ARS 10.8
Guidance: One method is to incorporate these requirements into the SSO's job description.		Related CSRs: 3.3.4, 2.2.17, 2.2.19
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.6 Retention procedures are established for all CMS sensitive information.	Review documents establishing the appropriate retention procedures.	HIPAA 164.316(b)(2)(i) CMS Directed
Guidance: Review retention procedures in relation to CMS PMs.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Entitywide Security Program Planning and Management***

General Requirement / Control Technique	Protocol	Reference
1.9.7 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.	Review documentation establishing that the required designations have been assigned with the considerations specified.	CMS Directed ARS 3.2 NIST 800-26 3.1.1
Guidance: Review the BPSSM and apply risk mitigation controls.		Related CSRs: 3.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.8 Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data verifying that vulnerability identification has been performed as specified. 3. Establish by inspection that the required summary lists are available.	PDD 63 333
Guidance: Review risk assessment.		Related CSRs: 1.8.9, 10.9.4, 1.8.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.9 The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting conduct of the required periodic reviews. 3. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.	FISCAM TSP-2.2 NIST 800-26 3.2.10 NIST 800-26 5.2 NIST 800-26 5.2.1
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.8.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.10 The system security plan establishes a security management structure with adequate independence, authority and expertise.	1. Verify by inspection that the system security plan contains the required management structure. 2. Review documentation supporting the assertion that the security management structure meets the stated requirements.	FISCAM TSP-3.1.1
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.5.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.9.11 Formal security and operational procedures and controls are documented.	1. Verify by inspection that the system security plan contains the required controls. 2. Review documentation supporting the security and operational controls.	NIST 800-26 12.2
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.4.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference

1.10 Security policies shall exist that address hiring, transfer, termination, and performance.

1.10.1 For perspective 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.

1. Inspect personnel records to confirm that references have been contacted and background checks have been performed.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documented conditions that allow access prior to completion of the screening process, as well as the in-place controls that compensate for allowing this type of access.

FISCAM TSP-4.1.1
CMS Directed
NIST 800-26 6.2
NIST 800-26 6.2.4

Guidance: As part of the HR function, develop a policy and procedure to address hiring, transfer, termination, and performance items.

Related CSRs: 1.1.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.10.2 Regular job or shift rotations are required for those personnel using sensitive information.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review staff assignment records to confirm that job and shift rotations occur.

FISCAM TSP-4.1.5
FISCAM TSD-1.1.7
NIST 800-26 6.1.6

Guidance: 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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.10.3 Regularly scheduled vacations exceeding several days are required for those personnel using sensitive information.

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.

FISCAM TSP-4.1.4
FISCAM TSD-1.1.7
NIST 800-26 6.1.6

Guidance: An approach is a policy developed that requires employees using sensitive information to take a minimum of 24 hrs continuous vacation.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.10.4 Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.

1. Review termination and transfer procedures for inclusion of the required processes.
2. 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.
3. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.

FISCAM TSP-4.1.6
HIPAA 164.308(a)(3)(ii)(C)
ARS 4.2
NIST 800-26 6.1.7

Guidance: These items need to be addressed as part of a HR Termination/Transfer procedure.

Related CSRs: 2.9.9, 2.2.20, 2.8.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
1.10.5 Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.	1. Review documentation establishing that reinvestigation policies for each position are consistent with the specified criteria. 2. Inspect personnel records to confirm sensitive position have had background reinvestigations performed within the required period.	FISCAM TSP-4.1.2

Guidance: CMS will provide future direction. Related CSRs: 2.5.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.10.6 Confidentiality or security agreements are required for CMS Business Partner Medicare employees and their contractors assigned to work with sensitive information.	1. Review policies on confidentiality or security agreements. 2. Determine whether confidentiality or security agreements are on file. 3. Review a sampling of agreements.	FISCAM TSP-4.1.3 HIPAA 164.314(a)(1) HIPAA 164.308(b)(1) HIPAA 164.308(b)(4) ARS 1.7 ARS 4.4 NIST 800-26 6.2.2

Guidance: One method would be to include the agreements as part of the procedural policy and include a standard contract clause for all procurements. Related CSRs: 1.11.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review Authorized Disclosure Agreements. 2. Review relevant policies for inclusion and directed use of the required directive.	IRS 1075 11.1@1 CMS Directed ARS 11.6

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. Related CSRs: 1.10.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 the electronically exchanged data. The CMS Business Partner will maintain a list of all contracts or other arrangements with other CMS Business Partners (include organization name and location, contract or agreement number, and purpose). The list of contracts will be provided to CMS in an MS Word document with the annual CAST submission.	1. Review documented arrangements/contracts for security content. 2. Verify risk-based decision is justified.	ARS 3.3 ARS 4.7 CMS Directed NIST 800-26 12.2.3

Guidance: A contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged should be completed prior to the exchange of data. Related CSRs: 1.5.8, 1.9.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.11.3 The CMS Business Partner has obtained satisfactory assurances that all external business associates will provide appropriate safeguards for CMS sensitive information.	1. Review the implemented safeguards. 2. Ensure satisfactory assurances have been provided.	HIPAA 164.308(b)(1) HIPAA 164.314(a)(1) ARS 10.8

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. Related CSRs: 2.14.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

1.11.4 Management has authorized interconnections 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.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review interconnected system agreements and established controls.	NIST 800-26 3.2.9 NIST 800-26 4.1.8

Guidance: Appropriate organizational officials should approve information system interconnection agreements. NIST SP 800-47 provides guidance on interconnecting information systems. Related CSRs: 2.14.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.12 Descriptions of Medicare operations, records, and assets are validated once a year.		
1.12.1 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.	Inspect the SSP and certification package for the required signatures.	CMS Directed NIST 800-26 1.2 NIST 800-26 5.1.1
Guidance: Review SSP certification package.	Related CSRs: 2.7.1	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
1.12.2 The safeguard selection decisions and the risk assessment reports are carefully analyzed to determine whether the security requirements in place adequately mitigate vulnerabilities.	Examine documentation supporting completion of the required review.	CMS Directed NIST 800-26 1.1.6
Guidance: Review risk assessment and safeguard selection for mitigation of risks and provide recommendations.	Related CSRs: 1.8.4	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
1.12.3 The CMS Business Partner is responsible for approving any necessary corrective action plans.	1. Review audit data supporting compliance with the required approval process. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. A plan of action is documented for correcting security deficiencies.	CMS Directed
Guidance: An approach is to provide annual sign-off, by senior management, on the Corrective Action Plan.	Related CSRs: 1.8.7, 1.2.1	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
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.	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. Review documentation supporting an assertion that the security system is fully documented. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-26 3.2.3 NIST 800-26 3.2.5
Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM.	Related CSRs: 1.9.4	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
1.13 General workstation security requirements shall be established.		
1.13.1 Policies and procedures are implemented that specify the proper workstation functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access CMS sensitive information.	1. Verify by inspection that the required policy/guideline is available. 2. Interview a sample to confirm familiarity with the required document.	HIPAA 164.310(b)
Guidance: One approach would be to address all the local workstations as well as the workstations used at home.	Related CSRs: 7.3.3, 7.3.4, 7.3.5, 7.4.1, 7.4.2, 7.5.1, 10.6.2	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
1.13.2 Controls prohibit employees from bringing their personally owned computer equipment and software into the workplace.	1. Review the specified policy. 2. Review the controls that prohibit this.	CMS Directed NIST 800-26 10.2.13
Guidance: Bringing personal computers into the workplace creates vulnerabilities to Medicare resources and could compromise sensitive data.	Related CSRs: 1.13.6, 1.13.7, 1.13.8, 2.2.28, 6.2.1	
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

Category: *Entitywide Security Program Planning and Management*

General Requirement / Control Technique	Protocol	Reference
1.13.3 All CMS-owned software (such as CAST) 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.	1. Interview programmers and system manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming enforcement of the required process.	CMS Directed
Guidance: No further guidance required.		Related CSRs: 10.7.1, 1.13.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.4 If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the process used to assure compliance with the required policy.	CMS Directed
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.		Related CSRs: 2.2.27
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	Determine the effectiveness of controlling portable devices by review business partner mobile computing policies.	CMS Directed NIST 800-26 7.3 NIST 800-26 7.3.2
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.		Related CSRs: 2.2.27
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.6 Users are prohibited from installing desktop modems.	1. Examine user's desktops for compliance. 2. War-Dialing. 3. Review the policy on addressing desktop modems.	ARS 6.5
Guidance: If no policy currently exists, one should be created. If no process for testing exists, one should be developed.		Related CSRs: 1.13.2, 10.8.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.7 The connection of portable computing or portable network devices on the CMS claims processing network is prohibited.	Review documentation restricting the use of portable devices.	ARS 6.4
Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.		Related CSRs: 1.13.2, 1.13.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.8 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.	1. Review existing policies and procedures to ensure prohibition of modems specified. 2. Review existing procedures to ensure sampling requirement defined sufficiently to ensure adequate coverage of all assets.	ARS 6.7
Guidance: Establish a policy prohibiting the connection or use of personal modems and develop procedure to ensure testing of all assets on a recurring basis.		Related CSRs: 1.13.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference

2. *Access Control*

2.1 Audit trails/logs shall be maintained.

2.1.1 User account activity audits are conducted using automated audit controls.

Protocol:
1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation describing the automated controls installed to implement the required process.
3. Inspect activity audit logs to confirm continuing use of the required process.

Reference: HIPAA 164.312(b); ARS 1.5; ARS 11.2; ARS 11.3; NIST 800-26 17.1.7

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 log data may be used to detect unauthorized activity and reduce volumes to manageable size.

Related CSRs: 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 4.2.1, 4.2.4, 3.1.5, 1.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.

Protocol:
1. 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.
2. Review documentation establishing that the computer systems processing sensitive information are secured from unauthorized access.
3. For a sample of hardware and software security features, obtain demonstrations of feature operation.
4. Review documentation describing how audit facilities are utilized to assure that everyone accessing a computer system containing sensitive information is accountable.

Reference: HIPAA 164.310(c); IRS 1075 5.6@4.1; IRS 1075 5.6@3.3; ARS 1.1; ARS 1.5; NIST 800-26 6.1.5; NIST 800-26 8.2.1; NIST 800-26 10.2.6

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.

Related CSRs: 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 2.2.16, 2.5.1, 2.2.32

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
2.1.3 All activity involving access to and modifications of sensitive or critical files is logged.	1. Validate the types of files involved and the features are turned on or coding has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. 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 logging methodology for each of these files. 4. Inspect samples of the specified audit logs to confirm continuing use of the required process.	FISCAM TAC-4.1 ARS 1.5 ARS 11.1 NIST 800-26 16.2.5 NIST 800-26 17.1

Guidance: Access control software is used to maintain an audit trail 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.

Related CSRs: 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, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.4 Access to audit trails/logs is restricted.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required restrictions. 3. Review security software settings and compare with system security policies and procedures. 4. Inspect a sample of audit log access lists.	CMS Directed NIST 800-26 17.1.3 NIST 800-26 17.1.4

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 logs.

Related CSRs: 2.10.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.5 The audit trail includes sufficient information to establish what events occurred and who or what caused them.	1. Review a sample of event logs and audit records to confirm the required content. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed ARS 11.2 ARS 11.3 NIST 800-26 15.2.1 NIST 800-26 17.1.1 NIST 800-26 17.1.2

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.

Related CSRs: 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, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.6 Audit trails/logs are reviewed periodically (i.e., minimum of weekly) and retained for a minimum of 60 days.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of audit data confirming that audit logs are being retained for the same period as the related claim.
3. Inspect a sample of audit data confirming that the required reviews have been conducted.

CMS Directed
HIPAA 164.308(a)(1)(ii)(D)
NIST 800-26 16.2.5
NIST 800-26 17.1.4
NIST 800-26 17.1.6

Guidance: Maintain, and periodically review, audit logs for critical application systems, including user-written applications. Audit logs may become evidence in legal proceedings, so care should be taken to protect their integrity

Related CSRs: 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, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 2.1.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.7 All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.

1. Inspect device configurations to confirm that all detected errors that can be logged are being logged.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Determine that audit logs have sufficient detail to assist with fault isolation and resolution of security abnormalities.

CMS Directed

Guidance: Audit trail 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 trail 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 trails 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.

Related CSRs: 4.1.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.1.8 Automated utilities are used to review audit logs daily for unusual, unexpected, or suspicious behavior. Manual reviews are performed randomly on demand, and at least once every 30 days.

1. Review audit review procedures.
2. Review audit logs.
3. Validate the system is operationally enabled.

ARS 11.5
NIST 800-26 17.1.7

Guidance: Procedures should exist which describe how to respond to an alert generated by the automated log review utilities.

Related CSRs: 2.1.6, 10.2.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 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. 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.

1. Review physical intrusion detection policies and procedures for spaces and rooms containing sensitive information for inclusion of the specified approach.
2. Review documentation describing measures used in conjunction with IDS to enhance protections provided directly by the IDS.

IRS 1075 4.3@24
FISCAM TAC-3.1.A.2
ARS 1.1
ARS 1.5

Guidance: Physical security controls used to detect access to facilities and protect them from intentional and unintentional loss or impairment.

Related CSRs: 3.6.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.2 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 trails and apparent security violations investigated and remedial action taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required controls. 3. Review a sample of audit data confirming consistent use of the required access process. 4. Inspect physical access audit trails to confirm that the physical accesses are being monitored.	IRS 1075 4.3@3 CMS Directed NIST 800-26 7.1.9

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.

Related CSRs: 2.8.6, 5.2.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.3 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.	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.	IRS 1075 4.3@2.2 CMS Directed

Guidance: Review BPSSM Section 4 for guidance.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.4 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.	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. Inspect a sample of audit data confirming that the secured area/perimeters are consistently secured at the end of working hours, and found secured when opened for business. 4. Confirm by inspection that the required electronic intrusion devices are in use.	IRS 1075 4.3@13 CMS Directed

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.

Related CSRs: 2.2.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.5 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.	If Security Rooms are used, review documentation confirming that each includes all of the required features.	IRS 1075 4.3@9 IRS 1075 4.3@10 IRS 1075 4.3@11 CMS Directed

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.

Related CSRs: 2.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.6 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.	IRS 1075 4.3@22 IRS 1075 4.3@23.1 IRS 1075 4.3@23.3 CMS Directed ARS 1.2

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.)

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.7 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.	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. 3. 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.	IRS 1075 4.3@1.3 CMS Directed

Guidance: Review BPSSM Section 4 for guidance.

Related CSRs: 1.1.8, 1.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.8 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.	1. Review facility security plan for procedures and policies for protection of sensitive information. 2. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of sensitive information data.	IRS 1075 4.3@19.2 IRS 1075 6.3@4 IRS 1075 4.3@19.4 CMS Directed
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.		Related CSRs: 6.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.9 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements. 3. Review documentation supporting the contention that the required process is followed for storage of sensitive information.	IRS 1075 4.3@16 CMS Directed
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.)		Related CSRs: 1.8.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.10 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.	Examine safe(s) or vault(s) for accompanying manufacturer documentation.	IRS 1075 4.3@18 CMS Directed
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.11 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of containers to confirm inclusion of the required features.	IRS 1075 4.3@15 CMS Directed
Guidance: A locked container is any metal container which is locked and to which keys and combinations are controlled.		Related CSRs: 1.8.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.12 Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.	Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.	HIPAA 164.310(c) ARS 1.1
Guidance: Workstations are located in controlled access areas and are safeguarded from unauthorized access.		Related CSRs: 2.8.6, 3.6.3, 7.3.3, 7.3.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.13 Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.	1. 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. Review documentation establishing the methods employed to deny access to sensitive information from unauthorized personnel during working hours.	HIPAA 164.310(a)(2(iii) IRS 1075 4.3@1.1 HIPAA 164.308(a)(3)(i)
Guidance: Procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.5.1, 2.5.3		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.14 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.	1. Review written emergency procedures for inclusion of the required process. 2. Inspect a sample of audit data confirming use of the required process.	FISCAM TAC-3.1.A.8 ARS 3.13 ARS 4.5 NIST 800-26 7.1.6
Guidance: Re-entry access methods are used to provide appropriate controls at emergency exits. Related CSRs: 5.6.2, 2.8.8		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.15 Procedures exist 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).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that the required process is consistently used.	HIPAA 164.312(d) HIPAA 164.308(a)(3)(i) HIPAA 164.310(a)(1) HIPAA 164.310(a)(2)(iii) ARS 3.13 ARS 7.22
Guidance: Policies and procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.4.2, 2.8.9, 2.8.3, 10.1.2		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.16 Access to facilities is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards or biometrics.	1. Review documentation designating specific individuals who are allowed access, and identifying the associated access control method used. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review a sample of audit data confirming consistent use of the required access process.	FISCAM TAC-3.1.A.3 PDD 63 711 ARS 1.1 ARS 1.3 NIST 800-26 7.1.1
Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties. Related CSRs: 1.3.15, 2.1.2, 2.5.4, 9.2.1, 2.9.4		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.17 Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of sign-in/sign-out registers to confirm collection of the required information. 3. Review a sample of audit data confirming compliance with the required register close out and review actions 4. Inspect a sample of audit data confirming monthly issue of a new AAL.	IRS 1075 4.3@4 HIPAA 164.308(a)(1)(ii)(D) HIPAA 164.310(a)(1) HIPAA 164.310(a)(2)(iii) IRS 1075 4.3@6 IRS 1075 4.3@8 HIPAA 164.312(d) FISCAM TAC-3.1.B.1 ARS 1.1 NIST 800-26 7.1.7
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.		Related CSRs: 1.9.5, 2.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.18 Management regularly reviews the list of persons with physical access to sensitive facilities.	1. Review a sample of audit data confirming periodic completion of the required reviews. 2. Review relevant policies and procedures for inclusion and directed use of the required process, and that they specify the review period.	FISCAM TAC-3.1.A.4 HIPAA 164.310(a)(2)(iii) NIST 800-26 7.1.2
Guidance: Access to sensitive facilities should be limited to personnel with a legitimate need for access to perform their duties.		Related CSRs: 2.8.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.19 Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	1. Review audit data confirming consistent use of the required procedure. 2. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.	FISCAM TAC-3.1.B.3 NIST 800-26 7.1.11
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.		Related CSRs: 1.4.1, 1.8.4, 1.9.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.20 Key combinations are changed 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.	1. Review audit data confirming consistent use of the required process. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 4.3@20.3 IRS 1075 4.3@20.6 HIPAA 164.308(a)(3)(ii)(C)
Guidance: There are 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.		Related CSRs: 1.10.4, 2.9.9, 2.8.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.2.21 All entry code combinations are changed periodically.	1. Review documentation and logs for entry code changes. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.1.B.2 NIST 800-26 7.1.8
Guidance: Periodically changing entry codes prevents reentry by previous employees or visitors who might have knowledge of the entry code.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement Control Technique	Protocol	Reference
2.2.22 Unissued keys or other entry devices are secured.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.	FISCAM TAC-3.1.A.7 NIST 800-26 7.1.5

Guidance: Unissued keys and other entry devices should be stored in appropriate security containers. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.23 Keys or other access devices are needed to enter the computer room and tape/media library.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming implementation and use of the required control.	FISCAM TAC-3.1.A.5 HIPAA 164.310(a)(2)(iii) NIST 800-26 7.1.4

Guidance: Access to these areas should be limited to personnel with a legitimate need for access to perform their duties. Related CSRs: 2.8.6, 10.1.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.24 Transmission and Storage of Data - Sensitive information may only be stored on hard disk as long as the CMS Business Partner approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades and are being used. Access control devices include: (1) password security; (2) audit trails/logs; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documentation of approval and installation of the required devices. 3. Review documentation confirming that the access control devices include the required features. 4. Review audit data confirming accomplishment of the required maintenance and upgrades, 5. Review audit data confirming consistent use of the required control devices.	IRS 1075 4.7@6 CMS Directed ARS 7.13 ARS 9.2

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. Related CSRs: 5.9.6, 5.12.1, 3.6.1, 2.9.17

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.25 Handling and Transporting Bulk Sensitive Information - Care is taken to safeguard sensitive information at all times. If hand carried between facilities, it is kept with an individual and protected from unauthorized disclosure. 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."	1. Review sensitive information handling and transporting policies and procedures for control technique compliance. 2. Review sensitive information transmittal forms for accuracy and completeness. 3. Inspect a sample of sensitive information data media for labeling compliance with the requirement.	CMS Directed ARS 9.7 NIST 800-26 8.2.4 NIST 800-26 8.2.5 NIST 800-26 8.2.6

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. Related CSRs: 1.3.3, 2.5.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.26 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data supporting continuing use of the required processes.	IRS 1075 4.4 HIPAA 164.310(d)(2)(iii) ARS 9.7

Guidance: The policies and procedures for protecting and transferring sensitive information materials with receipts ensure custody control and accountability during transfers. Related CSRs: 1.3.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.27 Alternate work site equipment controls are: (1) only CMS Business Partner-owned computers and software are used to process, access, and store sensitive information; (2) 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process by personnel working from their homes or alternate worksites. 2. Inspect documentation confirming that the required controls are implemented and consistently used.	IRS 1075 4.7@2 IRS 1075 4.7@3 IRS 1075 4.7@4.1 IRS 1075 4.7@5 CMS Directed

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. Related CSRs: 1.13.4, 1.13.5

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.

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.28 Responsibility is assigned and security procedures are documented for bringing 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.	Inspect documentation confirming that the required controls are implemented and consistently used.	HIPAA 164.310(d)(1) HIPAA 164.310(d)(2)(iii)

Guidance: The procedures for checking all hardware and software in to and out of the facility assist in maintaining an accurate inventory. Related CSRs: 1.13.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.29 Procedures are implemented to control access to software programs undergoing testing or revision.	Procedures are in place to protect CMS sensitive information during software testing and revisions.	HIPAA 164.310(a)(2)(iii)

Guidance: It is good practice to have an Security Test and Evaluation plan. Related CSRs: 6.4.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.30 Policies and procedures are implemented to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).	A maintenance tracking system should be implemented.	HIPAA 164.310(a)(2)(iv)

Guidance: It is a good practice to keep an inventory of resources. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.2.31 Boot access to removable media drives is disabled when not explicitly required. Removable media drives are removed when not explicitly required. System BIOS settings are locked and BIOS access is password-protected.	1. Review system configuration logs. 2. Examine access audit logs. 3. Randomly validate BIOS access is protected on desktops. 4. Review documentation on authorized removable media.	ARS 7.14

Guidance: Access to removable media drives should be tightly controlled. BIOS access should also be controlled. Related CSRs: 1.3.14, 1.5.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.2.32 Physical ports (e.g., wiring closets, patch panels, etc.) are disabled when not in use.	Review documentation requiring the disabling of physical ports.	ARS 1.10

Guidance: Policy should exist which defines the physical ports that are required for operation. Related CSRs: 2.1.2, 2.3.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	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.	FISCAM TAC-3.2.B

Guidance: It is important that all access paths (e.g., Internet, dial-in, telecommunications) be identified and controlled to eliminate "backdoor" paths. Related CSRs: 3.4.1, 4.5.1, 2.3.2, 10.8.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.3.2 All proxies not explicitly required are disabled and/or removed. Proxy access is granted only to those hosts, ports, and services that are explicitly required.	1. Review list of hosts, ports, and services to which proxy access is granted. 2. Review the policy statement.	ARS 6.3

Guidance: Hosts, ports, and services that are required should be explicitly identified. Related CSRs: 2.3.1, 2.2.32

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review documentation of the access control process to confirm inclusion of a procedure for emergency access. 2. Review documentation of the access control process to confirm inclusion of at least one of the required features.	HIPAA 164.312(a)(2)(ii) HIPAA 164.310(a)(1) HIPAA 164.312(a)(2)(i) ARS 5.5

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. Related CSRs: 5.2.7, 5.6.2, 2.9.12

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 and; (4) automatically terminated after a predetermined period.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that all four specified elements of the required process is consistently used.	FISCAM TAC-2.2 ARS 4.5 NIST 800-26 15.1.4

Guidance: As with normal access authorizations, emergency and temporary access should be approved and documented. Related CSRs: 5.2.7, 2.2.15, 2.8.3, 2.8.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	1. Inspect documentation identifying systems that process sensitive information. 2. Review documentation establishing that all computers in all specified systems meet requirements in their implemented configuration. 3. Review documentation of the configuration management process used to assure that all systems remain in certified configurations.	IRS 1075 5.7@2 CMS Directed
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.		Related CSRs: 2.2.13, 1.9.1, 2.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.2 Classifications and criteria have been established and communicated to resource owners.	1. Review policies specifying classification categories and related criteria to be used by resource owners in classifying their resources according to the need for protective controls. 2. Inspect audit data confirming that the required policy has been communicated to resource owners.	FISCAM TAC-1.1
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.		Related CSRs: 1.7.1, 2.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.3 Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation establishing that existing safeguards provide the required protections.	HIPAA 164.312(d) IRS 1075 6.3@7.1 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) PDD 63 711 ARS 7.22 ARS 10.8
Guidance: Policies and procedures limit access while ensuring that properly authorized access is allowed based on an employee's need-to-know.		Related CSRs: 2.12.1, 2.2.13, 2.7.2, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.4 Sensitive information is kept separate from other information to the maximum extent possible. Files are clearly labeled to indicate that sensitive information is included. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information.	1. Review sensitive information handling procedures for inclusion of the required processes. 2. For a sample of media and devices containing sensitive information, inspect to confirm use of the required labels.	IRS 1075 5.3@1.1 IRS 1075 5.3@2.1 IRS 1075 5.3@3.1 IRS 1075 5.3@3.2 CMS Directed ARS 9.3 NIST 800-26 8.2.5
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 log 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.		Related CSRs: 2.2.16, 1.3.15, 2.2.25
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.5.5 Every personnel position with access to CMS sensitive information processing is designated with a sensitivity level, and documentation is available to support the security and suitability standards for these personnel commensurate with their position sensitivity level and appropriate personnel investigation requirements.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample of personnel positions, inspect documentation establishing the associated sensitivity level.	CMS Directed PDD 63 711 NIST 800-26 6.1.1
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.		Related CSRs: 1.10.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.6 An 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 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 documentation verifying independent review includes interconnect system security controls.	IRS 1075 6.3@7.2 FISCAM TSP-5.1.2 NIST 800-26 2.1 NIST 800-26 2.1.1 NIST 800-26 2.1.2 NIST 800-26 3.2.6
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.		Related CSRs: 1.8.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.7 CMS Business Partner office facilities processing sensitive information are subjected to an annual self-assessment.	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.	CMS Directed IRS 1075 6.3@7.2 FISCAM TSP-5.1.1
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.		Related CSRs: 2.12.1, 1.4.2, 1.8.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.8 Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.	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.	HIPAA 164.316(b)(2)(i) IRS 1075 6.3@7.3.1 CMS Directed
Guidance: Inspection, self-assessment, and corrective action reports are an important means of identifying areas of noncompliance and remedial actions performed to correct noncompliance.		Related CSRs: 1.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.5.9 Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.	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.	CMS Directed IRS 1075 5.6@8
Guidance: The procedures are used to test the security system attributes.		Related CSRs: 1.4.2, 5.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.5.10 Sensitive information system development documentation is available, including security mechanisms and implementation.	Inspect system design and test documentation for an explanation of security mechanisms and how they are implemented.	FISCAM TCC-1.1.1

Guidance: The system development documentation provides security mechanism and implementation review guidance to staff with varying levels of skill and experience.

Related CSRs: 6.3.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.5.11 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.	Review the sensitive information system documentation for inclusion of required test documentation.	FISCAM TCC-2.1.1 FISCAM TCC-2.1.4 FISCAM TCC-2.1.8 NIST 800-26 12.1.5

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.

Related CSRs: 6.3.1, 6.3.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.6 Actual or attempted unauthorized, unusual, or sensitive access shall be monitored.

2.6.1 Security violations and activities, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.	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.	FISCAM TAC-4.2 ARS 10.6 ARS 11.1 NIST 800-26 11.2.6 NIST 800-26 16.1.10 NIST 800-26 17.1 NIST 800-26 17.1.8

Guidance: Audit functions should be activated to maintain critical audit trails and report unauthorized or unusual activity to the appropriate personnel.

Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 4.2.1, 4.2.4, 3.1.1, 10.2.3, 2.9.1, 10.2.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.6.2 Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.	1. Review documentation of the controls used to enforce this requirement. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed

Guidance: Audit trails 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 trail that logs 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 recorded in an audit log.

Related CSRs: 3.6.5, 5.2.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Confirm by inspection that the required procedures exist. 2. By inspection confirm that supervisors have specified procedures.	CMS Directed

Guidance: Procedures should be in-place to monitor visitors and contractors to insure they perform only authorized activities and work functions.

Related CSRs: 2.2.17

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	1. Review resource classification documentation and compare to risk assessments. 2. Inspect audit data confirming that the required approval and review processes are consistently used.	FISCAM TAC-1.2 PDD 63 711
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.		Related CSRs: 1.7.1, 2.5.2, 1.8.3, 4.4.1, 1.12.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	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.	IRS 1075 5.2@1.1 HIPAA 164.308(b)(1) HIPAA 164.308(a)(4)(ii)(C) IRS 1075 5.2@1.3 CMS Directed HIPAA 164.308(a)(4)(i) ARS 4.4 ARS 7.22
Guidance: The policies and procedures for limiting access ensure that properly authorized access is allowed based on an employee's need-to-know.		Related CSRs: 2.12.1, 2.5.3, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8 Resource owners shall identify authorized users and the level of authorization.		
2.8.1 Security is notified immediately when system users are terminated or transferred.	1. Review relevant policies and procedures for inclusion and directed use of the required procedure. 2. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.	FISCAM TAC-2.1.6
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.		Related CSRs: 1.10.4, 2.2.20, 2.9.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.2 All changes to security profiles by SSO or designated representative are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming routine identification and investigation of unusual activity. 3. Review a selection of recent profile changes and activity logs.	FISCAM TAC-2.1.5
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.		Related CSRs: 9.3.4, 2.11.4, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.3 SSOs or their designated representative review access authorizations and discuss any questionable authorizations with resource owners.	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.	FISCAM TAC-2.1.4 PDD 63 711 ARS 7.22
Guidance: One method is for a listings of authorized users and their specific access needs should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security manager.		Related CSRs: 1.4.1, 2.2.15, 2.4.2, 3.3.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.8.4 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a selection of users with dial-up access, review authorization and justification.	FISCAM TAC-2.1.3 ARS 7.11
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.		Related CSRs: 10.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
2.8.5 Owners periodically review access authorization listings and determine whether they remain appropriate.	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.	FISCAM TAC-2.1.2 PDD 63 711 NIST 800-26 15.2.2
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.		Related CSRs: 2.2.18, 1.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.6 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.	1. By inspection, confirm that authorization lists include the required information. 2. Inspect audit data confirming continuing maintenance of authorization lists and access controls for restricted areas.	CMS Directed
Guidance: Authorization lists and controls for restricted areas should be part of doing business to restrict access to areas containing or processing sensitive information.		Related CSRs: 6.4.1, 2.2.2, 2.2.12, 2.2.23
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.7 Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample representing each type of computer operating system, and for standalone and each mode of network connection affecting banner display, observe that the warning banner on the sample computer is consistent with the documented procedure.	IRS 1075 5.1@1.3 CMS Directed ARS 3.6
Guidance: The log-on banner/screen warning banner warns the user that the system processes sensitive information and it is subject to monitoring each time they log-on.		Related CSRs: 10.8.3, 10.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.8.8 Documented policies and procedures exist 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.	Review the appropriate documented policies and procedures for inclusion of the required rules.	HIPAA 164.312(a)(1) HIPAA 164.312(e)(1) HIPAA 164.308(a)(3)(i) ARS 4.5 ARS 11.7
Guidance: The policies and procedures used to grant different levels of access to sensitive information are based on an employee's need-to-know.		Related CSRs: 2.2.14
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.8.9 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to the SSO.	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.	FISCAM TAC-2.1.1 NIST 800-26 15.1.1

Guidance: Policies and procedures should exist for authorizing access to information resources and for documenting such authorizations. Related CSRs: 2.14.1, 2.2.15, 1.4.1, 2.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.

2.9.1 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 administrative reset.	1. Review security software password parameters. 2. Review pertinent policies and procedures. 3. Observe the system directed action in response to four invalid access attempts, confirming that the action is consistent with the documented policy.	FISCAM TAC-3.2.A.5 ARS 7.12 NIST 800-26 15.1.14

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. Related CSRs: 2.6.1, 7.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.2 Use of names or words as passwords is prohibited.	Review relevant policies for inclusion and directed use of the required prohibition.	FISCAM TAC-3.2.A.2

Guidance: 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. Related CSRs: 1.1.1, 3.6.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.3 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.	1. Interview a sample of users to confirm the required understanding and device possession. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.8

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. 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). 3. Review documentation describing audit systems implemented to record all accesses, including access scripts, to protected information. 4. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description. 5. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing. 6. Inspect a sample of access audit data supporting continuing use to the required process.	HIPAA 164.312(e)(1) IRS 1075 4.7@6 FISCAM TAC-3.2.A HIPAA 164.312(a)(1) ARS 9.2 NIST 800-26 15.1.3

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.

Related CSRs: 2.7.2, 2.2.16, 2.5.3, 2.11.4, 7.4.1, 7.4.2, 2.9.14

☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.9.5 When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) Authentication is provided through ID 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. 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.) 3. 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. 4. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.	IRS 1075 5.8@5.1 IRS 1075 5.8@5.2 IRS 1075 5.8@5.3 IRS 1075 5.8@5.4 FISCAM TAC-3.2.E.1 ARS 7.1 ARS 7.11 NIST 800-26 16.2.4

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.

Related CSRs: 3.6.1, 3.6.3, 10.8.2, 10.10.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.6 Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff after a predetermined amount of time (normally 15 minutes) and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), or (d) telephone callback procedure.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation supporting implementation of the required controls. 3. Review a sample of audit data confirming continuing use of the required controls.	HIPAA 164.312(a)(2)(iii) HIPAA 164.312(d) HIPAA 164.312(a)(2)(i) ARS 1.1 ARS 7.1 ARS 7.15 ARS 7.16 ARS 7.21 NIST 800-26 15.1

Guidance: Procedures should be in place to authenticate users before granting them access to the system or application.

Related CSRs: 7.3.5, 10.8.2, 10.10.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.9.7 Password files are encrypted.	1. View a sample dump of password files (e.g., hexadecimal printout). 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.7

Guidance: Encrypting the password file reduces the risk that it could be accessed and read by unauthorized individuals.

Related CSRs: 10.5.1, 2.9.16, 2.9.17

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.9.8 Vendor-supplied passwords are replaced immediately.	1. 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. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.3 NIST 800-26 15.1.13
Guidance: Vendor supplied passwords are known by every hacker and they are usually the first passwords tried by hackers.		Related CSRs: 3.6.2, 10.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.9 Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	1. Review pertinent policies and procedures. 2. Review documentation of such comparisons. 3. Interview security managers. 4. Make comparison using audit software.	FISCAM TAC-3.2.A.6 NIST 800-26 15.1.5
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.		Related CSRs: 1.10.4, 2.2.20, 2.8.1, 2.10.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.10 Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed every 60 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least 8 characters in length; (6) must include at least one number, one upper/lower case character, and one special character; and (7) prohibited from reuse for at least 6 generations.	1. Interview users. 2. Review security software password parameters. 3. Observe users keying in passwords. 4. Attempt to log on without a valid password. Make repeated attempts to guess passwords. 5. Assess procedures for generating and communicating passwords to users. 6. Review pertinent policies and procedures.	FISCAM TAC-3.2.A.1 CMS Directed HIPAA 164.308(a)(5)(ii)(D) FISCAM TAC-3.2.A.4 ARS 3.9 ARS 3.10 ARS 3.11 NIST 800-26 15.1.6 NIST 800-26 15.1.7 NIST 800-26 15.1.9
Guidance: Policies and procedures should exist that implement these minimum password requirements.		Related CSRs: 7.3.2, 10.10.1, 2.9.14
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.11 Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. 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.	1. Inspect a sample of workstations running each type of operating system in use to confirm that the required process is in use. 2. Review configuration documentation supported implementation of the required feature.	FISCAM TAC-3.2.C.3 CMS Directed HIPAA 164.310(b) ARS 7.15 ARS 7.16 NIST 800-26 16.1.4
Guidance: Workstation 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.		Related CSRs: 7.3.5, 10.10.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.12 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.	Review documentation establishing that authorization control exists, and includes the required feature.	HIPAA 164.308(a)(4)(ii)(B) ARS 11.6
Guidance: The mechanisms are used to authenticate users before granting them access permissions to the system or application.		Related CSRs: 2.4.1, 2.9.18
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

	General Requirement / Control Technique	Protocol	Reference
2.9.13	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.	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.	HIPAA 164.308(a)(4)(ii)(A)
	Guidance: Review security policies and procedures for business partner access.		Related CSRs: 1.4.6
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
2.9.14	System Administrators use unique UserIDs and passwords to perform administrator functions. These UserIDs are not shared with anyone and are different from the administrator's own personal UserID.	1. Ensure that System Administrators have unique UserID when performing admin functions. 2. Interview System Administrators regarding their UserIDs 3. Review usage reports to establish activity.	ARS 3.12
	Guidance: Available procedures define the usage of the unique UserIDs.		Related CSRs: 2.9.10, 2.9.4
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
2.9.15	Unique and separate administrator accounts are used for administrative versus non-administrative activities.	1. Ensure that System Administrators have unique UserID when performing admin functions. 2. Interview System Administrators regarding their UserIDs.	ARS 7.7
	Guidance: The use of unique and separate accounts helps to ensure that administrative activities are kept separate from non-administrative activities.		Related CSRs:
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
2.9.16	Highly sensitive system files are encrypted.	1. Verify that the designated files have been encrypted. 2. Develop criteria for identification of files that should be encrypted	ARS 7.18
	Guidance: Encryption of sensitive system files helps ensure that file access is limited. The encryption feature should be evaluated, implemented, and tested for protecting sensitive files. Highly sensitive system files may include, but are not limited to, password files, digital signature private keys, or other Business Partner-designated sensitive files.		Related CSRs: 2.9.7
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
2.9.17	Data are protected with system access controls and encrypted when residing in non-secure areas.	Review documentation confirming that the controls and encryption features are properly implemented in non-secure areas.	ARS 9.1 NIST 800-26 7.3.1
	Guidance: The robustness of protection provided should be commensurate with the sensitivity of the information.		Related CSRs: 2.2.24, 2.9.7
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
2.9.18	User identification is required for any transaction that has information security implications.	1. Review helpdesk procedures. 2. Interview helpdesk personnel to verify understanding of requirement.	ARS 3.5
	Guidance: Help desk policy should require individual identification before transactions can be completed.		Related CSRs: 2.9.12, 1.1.10
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
2.9.19	Controls are in place to determine compliance with password policies.	Review the procedures for determining compliance with password policies.	NIST 800-26 11.2.3
	Guidance: Procedures should exist to ensure compliance with password policies through review or testing.		Related CSRs:
	☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.9.20 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.	1. Review the policies and procedures for distributing passwords. 2. Review the policies and procedures for handling lost and compromised passwords.	NIST 800-26 15.1.10 NIST 800-26 15.1.11

Guidance: Users take reasonable measures to safeguard passwords, including not loaning or sharing passwords with others, and reporting lost or compromised passwords immediately.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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. Access to security software is restricted to security administrators only.	1. Review documentation describing the security software in use for restriction of access to data files and software programs. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of security software parameters that limit access to the security software to security administrators.	FISCAM TAC-3.2.C.1 FISCAM TAC-3.2.C.2 ARS 7.22 NIST 800-26 16.1.3

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.

Related CSRs: 3.6.4, 3.6.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Perform penetration testing by attempting to access and browse computer resources. 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. 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. 5. Review documentation describing the standardized naming conventions in use for resources.	FISCAM TAC-3.2.C.5 FISCAM TAC-3.2.C.6 ARS 7.9 NIST 800-26 16.1.2 NIST 800-26 16.1.6

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.

Related CSRs: 6.4.3, 6.4.4, 2.1.4, 3.6.5, 6.4.1, 6.8.2, 2.10.6

☐ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
2.10.3 Modification of data is restricted to authorized employees.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List(s) identifying employees who are authorized to update data. 3. Inspect a sample of audit data confirming that the required process is consistently used 4. Review documentation of the control used to restrict of data updating to authorized employees.	CMS Directed
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.		Related CSRs: 7.4.1, 7.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review documentation of the process used to provide the specified control over routines that modify the status of a file. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.	CMS Directed
Guidance: Utilities for file access and related processing need controls in place.		Related CSRs: 7.4.1, 7.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.10.5 Inactive user accounts are monitored and removed when not needed.	1. Review a sample of audit data confirming continued operation of the required control. 2. Review documentation describing how the required control is implemented.	FISCAM TAC-3.2.C.4 NIST 800-26 15.1.8 NIST 800-26 16.1.5
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.		Related CSRs: 2.9.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.10.6 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.	1. Validate security program system setup or rules (RAC-F/ACF2/TopSecret) or access setup in other operating systems. 2. Examine access in system audit logs.	ARS 7.3 NIST 800-26 16.3
Guidance: It is important that the OS controls are implemented to disable public read and write access to sensitive information.		Related CSRs: 1.9.3, 2.10.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.11 Logical controls shall be implemented for databases and DBMS software.		
2.11.1 Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	1. Review security system parameters. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.D.4
Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
2.11.2 Access and changes to DBMS software are controlled.	1. Review the controls protecting DBMS software. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.D.3 HIPAA 164.310(a)(2)(iii)

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.

Related CSRs: 6.5.2, 6.6.1, 3.4.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.11.3 Use of DBMS utilities is limited.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List for DBMS utilities to confirm access is limited to those personnel have an operational requirement for access.	FISCAM TAC-3.2.D.2

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 trails.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.11.4 Database management systems (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) control access to the data dictionary using security profiles and passwords; (3) maintain audit trails/logs that allow monitoring of changes to the data dictionary; and (4) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.	1. Interview database administrator. 2. Test controls by attempting access to restricted files. 3. Review pertinent policies and procedures.	FISCAM TAC-3.2.D.1 ARS 11.2 ARS 11.3 NIST 800-26 16.1.9

Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. Data dictionary software, which interfaces with the DBMS and provides a method for documenting elements of a database, may also provide a method of securing data. In addition, use of the DBMS and data dictionary should be protected through the use of logical access controls and audit trails.

Related CSRs: 6.3.5, 6.6.1, 2.8.2, 2.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	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.	IRS 1075 6.3@5 PDD 63 193 ARS 3.2

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.

Related CSRs: 1.4.2, 2.5.3, 2.5.7, 2.7.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

2.12.2 Medicare data are not released to outside personnel unless the personnel are authorized to receive the data and their identity is verified.	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.	CMS Directed

Guidance: There should be procedures used to verify that outside personnel who request Medicare data are authorized to receive the data before releasing it.

Related CSRs: 1.3.2, 1.3.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Access Control*

General Requirement / Control Technique	Protocol	Reference
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.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.	FISCAM TAC-4.3.1 FISCAM TAC-4.3.2 NIST 800-26 7.1.10
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.		Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.13.2 Violations are summarized and reported to senior management.	1. Interview senior management and personnel responsible for summarizing violations. 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.	FISCAM TAC-4.3.3
Guidance: 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.		Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.13.3 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	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.	FISCAM TAC-4.3.4
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.		Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.2, 3.1.1, 3.4.1, 1.2.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.13.4 Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.	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.	IRS 1075 3.2@2.4 CMS Directed
Guidance: The process of inventorying and documenting missing tapes containing sensitive information should be integrated into the normal business processes of the organization.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect standard approval forms.	FISCAM TAC-2.3.1
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.		Related CSRs: 1.3.8, 2.8.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

2.14.2 Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Examine documents authorizing file sharing and file sharing agreements.

FISCAM TAC-2.3.2
NIST 800-26 16.2.7

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.

Related CSRs: 1.11.3, 1.11.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.

Review system operational policies and guidelines.

FISCAM TSS-2.2.2
NIST 800-26 11.2.2

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.

Related CSRs: 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 2.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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).

Determine when the last management review was conducted, and analyze their review regarding the intended functioning of software monitoring control techniques and controlling risk.

FISCAM TSS-2.2.4
ARS 7.5

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.

Related CSRs: 6.3.10, 1.5.5, 1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.9.7, 2.13.3, 4.4.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.1.3 The use of privileged system software and utilities is reviewed by technical management.

1. Interview technical management regarding their reviews of privileged system software and utilities usage.
2. Review documentation supporting technical management reviews.
3. Review documentation for system software utilities and verify that technical management has given use approvals.
4. 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 user ID`s for performing privileged and normal activities? - Are the login privileges for highly privileged accounts available only from console and terminals situated within the console room ? - Is the audit trail maintained of activities conducted by highly privileged users? How long is it preserved?

FISCAM TSS-2.2.1
ARS 7.4

Guidance: Privileged access may be used only to perform assigned job duties.

Related CSRs: 1.8.4, 3.3.3, 4.1.3, 4.3.1, 4.6.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***System Software***

General Requirement / Control Technique	Protocol	Reference
3.1.4 Systems programmers' activities are monitored and reviewed.	1. Determine that system programmer supervisors are supervising and monitoring their staff. 2. Review documentation supporting the supervising and monitoring of systems programmers' activities. 3. 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.	FISCAM TSS-2.2.3 ARS 7.6 ARS 7.8

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 logon 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.

Related CSRs: 4.2.1, 4.2.4, 3.2.3, 4.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.1.5 Systems support alarm features to provide immediate notification of predefined events.	1. Review security plan to determine use of audit logs and alarms set points. 2. Review audit logs.	HIPAA 164.312(b)

Guidance: It is a good practice to have an automated audit system perform the immediate notification.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Verify that the appropriate responsibilities have been defined. 2. Interview systems programmers regarding their responsibilities.	FISCAM TSS-2.1.2 NIST 800-26 10.1.5

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.

Related CSRs: 1.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.2.2 Responsibilities for monitoring use are defined and understood by technical management.	1. Verify that the appropriate responsibilities are defined. 2. Interview technical management regarding their responsibilities.	FISCAM TSS-2.1.3

Guidance: Security training is adjusted to the level of the technical management's responsibilities.

Related CSRs: 1.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *System Software*

General Requirement / Control Technique	Protocol	Reference
3.2.3 Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	1. Interview management and systems personnel. 2. Verify the existence and current version of the appropriate policies and procedures.	FISCAM TSS-2.1.1

Guidance: 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.

Related CSRs: 3.1.4, 4.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.2.4 The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	1. Determine whether logging occurs and what information is logged. 2. Review logs. 3. Using security software reports, determine who can access the logging files.	FISCAM TSS-2.1.4 NIST 800-26 10.1.5

Guidance: The output report log 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.

Related CSRs: 1.9.4, 9.6.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review pertinent policies and procedures. 2. Interview management and system personnel regarding access restrictions. 3. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. 4. Attempt to access the operating system and other system software.	FISCAM TSS-1.1.2

Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses.

Related CSRs: 1.1.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.3.2 Policies and procedures for restricting access to systems software exist and are up-to-date.	1. Interview management and systems personnel regarding access restrictions. 2. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. 3. Attempt to access the operating system and other system software. 4. Review pertinent policies and procedures.	FISCAM TSS-1.1.1

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.

Related CSRs: 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of system programmers were reviewed.	FISCAM TSS-1.1.4

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 logs. 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.

Related CSRs: 3.1.3, 1.1.2, 2.8.3, 4.6.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *System Software*

General Requirement / Control Technique	Protocol	Reference
3.3.4 Justification and management approval for access to systems software is documented and retained.	1. Interview system manager and security administrator. 2. Review appropriate documentation, and verify that it is retained.	FISCAM TSS-1.1.3

Guidance: 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. Related CSRs: 1.9.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.4 Installation of system software shall be documented and reviewed.

3.4.1 Installation of all system software is logged to establish an audit trail/log and is reviewed by data center management.	1. Interview data center management about their role in reviewing system software installations. 2. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.	FISCAM TSS-3.2.4

Guidance: A good process for monitoring and documenting migration of system software is in the change management process for the organization. Related CSRs: 9.7.1, 9.8.1, 9.8.2, 9.8.3, 6.5.2, 2.3.1, 2.11.2, 2.13.3, 4.7.6, 6.3.5, 6.3.6, 6.3.10, 6.6.1, 6.7.1, 6.8.1, 10.7.3, 10.10.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.4.2 Migration of tested-and-approved system software to production use is performed by an independent library control group.	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.	FISCAM TSS-3.2.2

Guidance: A good process for monitoring and documenting the migration of system software is in the change management process for the organization. Related CSRs: 6.8.2, 4.7.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.4.3 Vendor-supplied system software includes software documentation and is supported by the vendor.	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.	FISCAM TSS-3.2.5 NIST 800-26 12.1.1 NIST 800-26 12.1.2

Guidance: A good approach is to include vendor maintenance with the purchase of the software. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.4.4 Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	1. Interview management and systems programmers about scheduling and giving advance notices when system 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.	FISCAM TSS-3.2.1

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. Related CSRs: 5.9.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement Control Technique	Protocol	Reference
3.4.5 Outdated versions of system software are removed from production libraries.	Review supporting documentation from a few system software migrations and the removal of outdated versions from production libraries.	FISCAM TSS-3.2.3

Guidance: 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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.4.6 All system software is current and has current and complete documentation.	1. Review documentation and test whether recent changes are incorporated. 2. Interview management and system programmers about the currency of system software, and the currency and completeness of software documentation.	FISCAM TSS-3.2.6

Guidance: An automated version tracking system can assist with tracking the current version of software and the software's documentation.

Related CSRs: 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

3.5 System software changes shall be authorized, tested and approved before implementation.

3.5.1 New system components and software versions or products and modifications to existing system software are tested and the test results are approved before implementation.	1. Determine the procedures used to test and approve system components and software prior to its implementation. 2. Select a few recent system component and software changes and review audit data confirming that the specified process was followed. 3. Review procedures used to control and approve emergency changes. 4. Select some emergency changes to system components and software, and test whether the indicated procedures were used.	FISCAM TSS-3.1.4 NIST 800-26 10.2 NIST 800-26 10.2.2

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.

Related CSRs: 5.7.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Interview management and systems personnel. 2. Verify that policies and procedures are current, and contain the required information. 3. Review the mission/business impact analysis documentation.	FISCAM TSS-3.1.1 NIST 800-26 1.2.2 NIST 800-26 10.2.1

Guidance: Usually, the change request will contain most of the selection, installation, modification, and cost information.

Related CSRs: 1.9.4, 1.4.1, 1.8.4, 4.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *System Software*

General Requirement Control Technique	Protocol	Reference
3.5.3 Procedures exist for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.	1. Review procedures for identifying and documenting system software problems. 2. Interview management and systems programmers. 3. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.	FISCAM TSS-3.1.2
Guidance: A good approach is to automate the software problem tracking processes. Monthly tracking reviews will assist in controlling any issues.		Related CSRs: 1.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.5.4 New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.	1. Determine what authorizations and documentation are required prior to initiating system software changes. 2. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.	FISCAM TSS-3.1.3
Guidance: A preformatted change request process provides efficiency and assists in the accuracy of the change tracking processes.		Related CSRs: 6.6.1, 6.7.1, 4.7.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.5.5 Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.	Verify the existence of checkpoint and restart capabilities.	CMS Directed
Guidance: Checkpoints and Restart capabilities on jobs will assist in meeting performance goals.		Related CSRs: 4.7.6
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.5.6 Procedures exist 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.	1. Interview an independent IT supervisor who has previously reviewed changes. 2. Verify the existence of emergency change procedures. 3. Interview system managers.	FISCAM TSS-3.1.5
Guidance: A good approach is to include emergency procedures in the change management process as well as appropriate procedures in the Contingency Plan		Related CSRs: 5.6.2, 5.7.2, 6.6.1, 1.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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 logged by automated logging facilities.	Review sample accesses to system software files to confirm automated logging facilities.	FISCAM TSS-1.2.2
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 logging or file changes occur.		Related CSRs: 2.2.24, 2.9.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
3.6.2 All vendor-supplied default logins, passwords, and security parameters have been disabled or reinitialized to more secure settings.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Test for default presence using vendor standard IDs and passwords.	FISCAM TSS-1.2.3 ARS 7.2 NIST 800-26 16.2.12 NIST 800-26 16.2.3
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.		Related CSRs: 2.9.8, 1.9.4, 10.10.1, 2.9.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *System Software*

General Requirement / Control Technique	Protocol	Reference
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.	1. Determine what terminals are set up as master consoles and what controls exist over them. 2. 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.	FISCAM TSS-1.2.4

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.

Related CSRs: 1.9.4, 2.2.12, 2.9.5, 10.10.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
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.	1. Obtain a list of all system software on test and production libraries used by the entity. 2. Verify that access control software restricts access to system software. 3. Using security software reports, determine who has access to system software files, security software, and logging files. Reports should be generated by the auditor, or at least in the presence of the auditor. 4. 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.	FISCAM TSS-1.2.2 HIPAA 164.310(a)(2)(iii)

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.

Related CSRs: 2.10.1, 1.1.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
3.6.5 The operating system is configured to prevent circumvention of the security software and application controls.	1. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods. 2. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.	FISCAM TSS-1.2.1 NIST 800-26 10.1.4

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.

Related CSRs: 2.10.1, 2.10.2, 2.2.1, 2.6.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
3.6.6 The operating system's operational status and restart integrity is protected during and after shutdowns.	1. Interview the system manager. 2. Verify the protection of the operating system during and after shutdowns.	CMS Directed

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.

Related CSRs: 5.2.9

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
3.6.7 All system defaults are reset after being restored from a backup.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify through testing or procedure reviews that system defaults are reset after being restored from a backup.	NIST 800-26 9.2.8

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.

Related CSRs: 5.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4. *Segregation of Duties*

4.1 Formal procedures shall guide personnel in performing their security duties.

4.1.1 Application-run manuals provide instruction on operating specific applications, including in-house applications.	1. Inspect run manuals for inclusion of the required instructions. 2. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-3.1.3 NIST 800-26 12.1.3

Guidance: Manuals should include instructions on job setup, console and error messages, job checkpoints, transaction logs, and restart and recovery steps after system failure.

Related CSRs: 4.1.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.1.2 Operators are prevented from overriding file labels or equipment error messages.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing how controls meet the specified requirement. 3. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-3.1.4

Guidance: A good approach is to provide periodic training in operating procedures, which should cover operator-prohibited activities.

Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.1.3 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.	1. Determine that the required operator and security manuals exist, and that they provide the required documentation. 2. Determine that documents are understood and adhered to by staff.	FISCAM TSD-3.1.2 NIST 800-26 12.1 NIST 800-26 12.1.7

Guidance: Manuals should contain instructions on all procedures which the employee is expected to perform on a regular basis and in an emergency situation.

Related CSRs: 5.6.2, 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 4.1.1, 3.1.3, 3.1.5, 2.1.7, 4.2.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.1.4 The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing use of the specified approval process.	CMS Directed

Guidance: The approval process should be documented and reviewed periodically.

Related CSRs: 3.5.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Segregation of Duties***

General Requirement Control Technique	Protocol	Reference
4.1.5 Duties in critical or sensitive control and financial functions are split to ensure least privileged and individual accountability.	1. Interview supervisors in the critical and sensitive control and financial areas. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-26 6.1 NIST 800-26 6.1.3

Guidance: Duties should be documented in job descriptions. Appropriate separation of data will assist in preventing fraud. See BPSSM information on fraud protective measures. Related CSRs: 4.3.1, 4.7.2

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.2 Active supervision and review shall be provided for all personnel.

4.2.1 All operator activities on the computer system are recorded on an automated history log.	1. Determine by review that an automated history log exists on each computer system, and that they record all operator activities. 2. Interview supervisors to confirm that supervisors routinely review history log.	FISCAM TSD-3.2.2

Guidance: The history log serves as an audit trail and should be reviewed routinely by supervisors. Related CSRs: 2.1.1, 2.6.1, 3.1.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.2.2 Personnel are provided adequate supervision and review, including each shift of computer operations.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing supervision and review in accordance with the documented process.	FISCAM TSD-3.2.1

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. Related CSRs: 1.4.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Interview supervisors and subordinate personnel to confirm continuing use of the required process. 2. Observe system startup. 3. Review audit data confirming that only authorized personnel are involved in the system startup operation. 4. Review audit data confirming that parameters set during IPL are consistently in accordance with documented procedures.	FISCAM TSD-3.2.4

Guidance: IPL establishes the environment in which the computer operates. System startup should be monitored to ensure that security features are enabled. Related CSRs: 4.1.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Segregation of Duties***

General Requirement / Control Technique	Protocol	Reference
4.2.4 Supervisors routinely review the history log and investigate any abnormalities.	1. Determine, by review supervisor's job description that this is included in the job description. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review history log for signatures indicating supervisory review. 4. Inspect a sample of documentation of the supervisor's investigative process.	FISCAM TSD-3.2.3
Guidance: The history log serves as an audit trail.		Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 2.1.1, 2.6.1, 3.1.4, 3.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

4.3 Job descriptions shall be documented.

4.3.1 Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	1. Review documentation establishing that existing documented job descriptions meet segregation of duty principles. 2. Inspect the effective dates of position descriptions to confirm that they are current. 3. Confirm by interview of the incumbents that documented job descriptions match actual current responsibilities and duties.	FISCAM TSD-1.2.1 NIST 800-26 6.1.2
Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.		Related CSRs: 3.1.3, 4.1.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Confirm by review that job descriptions are documented, and that they meet the specified criteria. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSD-1.2.2
Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.		Related CSRs: 5.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

4.4 Management shall review 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).	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.	FISCAM TSD-2.2.2
Guidance: A good approach is a documented management review on an annual basis.		Related CSRs: 3.1.2, 2.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.4.2 Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.	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.	FISCAM TSD-2.2.1
Guidance: A periodic employee performance review could be used to demonstrate compliance.		Related CSRs: 3.1.4, 3.2.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Segregation of Duties***

General Requirement / Control Technique	Protocol	Reference
4.5 Physical and logical access controls shall be established.		
4.5.1 Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	Review documentation establishing now physical and logical access controls accomplish the specified restriction.	FISCAM TSD-2.1 CMS Directed NIST 800-26 15.2 NIST 800-26 16.1
Guidance: This can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities.		Related CSRs: 2.3.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.6 Employees shall understand their security duties and responsibilities.		
4.6.1 All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	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.	FISCAM TSD-1.3.1 ARS 3.1
Guidance: Employees should have access to their job descriptions and discuss during their performance evaluations.		Related CSRs: 3.1.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	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.	FISCAM TSD-1.3.2 ARS 5.1
Guidance: Senior management is responsible for assuring that employees understand their responsibilities.		Related CSRs: 1.2.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.	1. Review documented procedures identifying responsibilities for restricting access by job position in key operating and programming activities to confirm that these responsibilities are clearly defined. 2. Interview a sample of personnel identified as having the specified responsibilities to confirm that the responsibilities assigned are clearly understood and followed. 3. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-1.3.3
Guidance: A good approach is to develop a matrix identifying resources in relation to organizational access and job title.		Related CSRs: 3.3.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	Review approval controls.	FISCAM TSD-1.1.4
Guidance: Compensating controls should be documented.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Segregation of Duties*

General Requirement / Control Technique	Protocol	Reference
4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. No individual has complete control over incompatible transaction processing functions.	1. Review the required analyses for inclusion of the specified elements. 2. Confirm by review that the required analyses reflect current operations.	FISCAM TSD-1.1.3

Guidance: Establish independent organizational groups with defined functions. Functions and related tasks performed by each unit should be documented. Related CSRs: 4.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.	1. Review documentation of process design establishing the specified separation of duties. 2. Confirm through interview, observation, and review of job descriptions for a sample of personnel, that these separation of duties requirements are met. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSD-1.1.5

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. Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.7.4 Policies and procedures for segregating duties exist and are up-to-date.	Confirm through inspection that the required policies and procedures exist and are consistent with current operations.	FISCAM TSD-1.1.1

Guidance: Policies are documented, communicated, and enforced. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.7.5 Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Confirm by review that documented operating procedures meet the required criteria.	FISCAM TSD-1.1.6

Guidance: Documentation should be reviewed periodically and updated as needed. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

4.7.6 Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) quality assurance/testing; (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.	1. Review the agency organization chart showing IS functions and assigned personnel. 2. Interview selected personnel and determine whether functions are appropriately segregated. 3. Review relevant alternative or backup assignments and determine whether the proper segregation of duties is maintained. 4. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.	FISCAM TSD-1.1.2 NIST 800-26 6.1.4 NIST 800-26 17.1.5

Guidance: Manuals and job descriptions include support functions of each individual. Related CSRs: 3.4.1, 3.4.2, 3.5.4, 3.5.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5. *Service Continuity*

5.1 Adequate environmental controls shall be implemented.

5.1.1	Building plumbing lines are known and do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known.	1. Examine facility maintenance records for history of water damage. 2. Interview site managers for knowledge of potential pumping related hazards and familiarity with mitigation procedures. 3. Interview a sample of operations staff to confirm familiarity with mitigation procedures for potential plumbing related problems. 4. Observe the operation, location, maintenance, and access to the air cooling systems condensate drains. 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. Review relevant procedures for inclusion mitigation measures for any potential plumbing related problems. 7. Review the current risk assessment to confirm investigation of the potential for plumbing related problems, and review risk mitigation plans for any such risks identified.	FISCAM TSC-2.2.4 ARS 1.9 NIST 800-26 7.1.17

Guidance: The SSO should work in conjunction with the building engineer/maintenance. Related CSRs: 5.6.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.2	Any behavior that may damage computer equipment is prohibited.	1. Review the risk assessment for identification of potentially hazardous employee activities. 2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment. 3. Review job descriptions to ensure there is guidance contained relative to destructive behavior.	FISCAM TSC-2.2.7

Guidance: Management should include behavioral guidance. For example keeping cans of coke on top of a PC could damage it. Related CSRs: 4.3.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.3	Controls have been identified to sufficiently mitigate identified risks and other disasters, such as floods, earthquakes, fire, etc.	1. Review the risk assessment plan for consideration of the specified potential risks. 2. Review documentation of efforts to identify additional risks specific to the region, area, or facility. 3. Review documentation of risk mitigation planning covering all identified risks. 4. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.	FISCAM TSC-2.2.2 ARS 1.9 NIST 800-26 1.2.3 NIST 800-26 7.1.19

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. Related CSRs: 1.8.4, 2.2.14, 5.6.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.1.4 Environmental controls are periodically tested.	1. Review the test plans for future tests. 2. Review test policies. 3. Review documentation supporting recent tests of environmental controls.	FISCAM TSC-2.2.6 ARS 1.9

Guidance: There should be a test plan for the testing of the environmental controls, e.g., humidistat. Related CSRs: 5.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.5 Redundancy exists in the air cooling system.	1. Review facility design documentation confirming air cooling system redundancy. 2. Review maintenance records confirming primary and redundancy systems are operational. 3. Observe demonstrations of operation of primary and redundant cooling systems. 4. Review policy and procedures relevant to operation and maintenance of primary and redundancy air cooling systems	FISCAM TSC-2.2.3 NIST 800-26 7.1.15

Guidance: Only the critical components or subsystems of the entire air cooling system need to be redundant. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.6 Fire suppression and prevention devices have been installed and are working (e.g., smoke detectors, fire extinguishers, and sprinkler systems).	1. Review facility drawings and other documentation documenting types and locations of the specified devices. 2. Review documentation of periodic inspections and maintenance of the specified devices and related systems to assure they are fully operational. 3. Review documentation supporting the qualifications of personnel inspecting and maintaining the specified devices and systems. 4. Observe that fire extinguishers, smoke detectors and sprinkler systems are in place and appear to be in working order.	FISCAM TSC-2.2.1 ARS 1.9 NIST 800-26 7.1.12

Guidance: A good approach is to have the fire department review the systems. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.1.7 An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down.	1. Review facility documentation confirming installation of an uninterruptible power system (UPS). 2. Review design and test data supporting the capacity of the system to support the facility technical load long enough to allow shut down with lose of no more that transactions in progress at the time primary power is lost. 3. Review documentation supporting existence of periodic test, and preventive maintenance consistent with system specifications. 4. Review policies and procedures for orderly shut down of the system within the time allowed by the available UPS capacity. 5. Interview a sample of operations personnel for familiarity with the orderly shut down process and applicable documented procedures. 6. Review documentation supporting periodic test of the orderly shut down process. 7. Observe that secondary power supplies exists.	FISCAM TSC-2.2.5 ARS 1.8 NIST 800-26 7.1.18

Guidance: The facility managers should periodically verify the current computing power load and auxiliary requirements for change. Related CSRs: 5.9.8, 5.10.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.8 Possible fire ignition sources, such as electronic devices or wiring, storage of combustible materials, and arson possibilities, are reviewed periodically.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review documentation of periodic inspections and storage of combustible materials.	NIST 800-26 7.1.13

Guidance: A good approach is to have the fire department review for possible fire ignition sources. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.1.9 Electric power distribution, heating plants, water, sewage, and other utilities are periodically reviewed for risk of failure.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review documentation supporting recent reviews of environmental controls.	NIST 800-26 7.1.16

Guidance: There should be a process for the testing of the environmental controls and periodic reviews for risk of failure. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.2 A Contingency Plan shall be documented in accordance with the CMS Business Partners Systems Security Manual.

5.2.1 The Contingency Plan provides for backup personnel so that it can be implemented independent of specific individuals.	1. Review the contingency plan to confirm inclusion of the specified provision. 2. Review documentation supporting timely availability of the backup personnel required by the contingency plan. 3. Talk with a random small sample of the designated backup persons to ensure that they understand their role in a contingency.	FISCAM TSC-3.1.2

Guidance: Refer to Appendix B of the BPSSM. Related CSRs: 5.8.1, 5.10.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.2.2 User departments have developed adequate manual processing procedures for use until automated operations are restored.	1. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation. 2. Review the contingency plan for identification of the specified manual procedures. 3. Inspect the required manual procedures for consistency with the contingency plan. 4. Interview the relevant process managers to confirm familiarity with the required procedures. 5. Review test reports to determine that manual procedures have been tested, at least on a sample basis.	FISCAM TSC-3.1.3
Guidance: Determine that the manual procedures have been tested. Refer to Appendix B of the BPSSM.		Related CSRs: 1.8.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.3 The Contingency Plan clearly assigns responsibilities for recovery.	Review the Contingency Plan to confirm clear identification of specific responsibilities for all elements of recovery.	FISCAM TSC-3.1.1 NIST 800-26 9.2.2
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.		Related CSRs: 3.6.4, 4.3.1, 4.6.1, 5.6.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.4 Contingency Plans consist of all components listed in the CMS Business Partners Systems Security Manual, Appendix B, and include detailed instructions for restoring operations.	1. Review Appendix B of the Business Partners Systems Security Manual. 2. Verify through inspection that the Contingency Plan includes the specified elements.	CMS Directed HIPAA 164.310(d)(1) FISCAM TSC-3.1.1 HIPAA 164.308(a)(7)(ii)(C) HIPAA 164.308(a)(7)(ii)(D) HIPAA 164.308(a)(7)(ii)(E) HIPAA 164.308(a)(7)(i) HIPAA 164.308(a)(7)(ii)(A) NIST 800-26 9.2.3 NIST 800-26 12.2.2
Guidance: A business partner Contingency Plan contains the topics described in Appendix B of the Business Partners Systems Security Manual.		Related CSRs: 5.3.1, 5.4.1, 5.4.2, 5.5.1, 5.6.1, 5.8.1, 3.6.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.5 Management, the SSO, and key affected parties approve Contingency Plans.	1. Verify through inspection that all Contingency Plans have been approved by management, SSO, and key affected parties. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-3.1.1 CMS Directed NIST 800-26 9.2.1
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.		Related CSRs: 5.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement / Control Technique	Protocol	Reference
5.2.6 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.	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.	FISCAM TSC-3.1.1 CMS Directed ARS 1.9 ARS 10.8
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.		Related CSRs: 5.5.1, 5.6.1, 5.6.2, 5.6.3, 5.6.4, 5.10.1, 2.6.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.7 The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.	Review the Contingency Plan emergency response procedures for inclusion of the required provision.	CMS Directed HIPAA 164.308(a)(7)(ii)(C) ARS 1.9
Guidance: Ensure that this immediate entry action has been practiced during exercises and training.		Related CSRs: 1.1.7, 2.4.1, 2.4.2, 5.6.1, 5.6.4, 2.2.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.8 Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency plans are re-evaluated before proposed changes are approved.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming that contingency plans have been reevaluated before any proposed major modifications were approved.	CMS Directed
Guidance: Change control management should provide for updates to the Contingency Plan.		Related CSRs: 5.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.9 Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.	1. Review documentation supporting the contention that existing contingency plans protect storage media from improper modification in the event of 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 describing use of software procedures to reduce the potential for data loss and/or modification during a system failure.	CMS Directed NIST 800-26 12.1.9
Guidance: Throughout documentation review and testing, ensure that the safeguards protect data from modification if the system fails.		Related CSRs: 2.5.1, 2.14.2, 3.6.6, 6.4.1, 7.2.2, 9.3.3, 9.8.1, 5.11.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.2.10 The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.	1. Review test reports. 2. Verify through inspection that the contingency plan identifies the specified interfaces.	CMS Directed
Guidance: Critical interfaces should be tested when the contingency plan is exercised.		Related CSRs: 5.3.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
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.	1. Verify by inspection that the required, prioritized list has been prepared. 2. Verify by inspection that the list is approved by senior management. 3. Review documentation supporting the contention that the list reflects current conditions. 4. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-1.1 HIPAA 164.308(a)(7)(ii)(E) NIST 800-26 9.1.3
Guidance: It is important to know what critical data and operations are needed to continue critical functions in an emergency. Related CSRs: 1.9.7, 2.1.3, 5.4.4, 5.8.1, 5.2.10		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.3.2 There are network diagrams and documentation on setups of routers and switches.	1. Verify by inspection that the required diagrams and setup documentation has been prepared. 2. Review relevant policies and procedures for inclusion of the stated requirements.	NIST 800-26 12.1.4
Guidance: It is important to have network diagrams and documentation on router and switch setups to restore critical functions in an emergency. Related CSRs:		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.4 Data and program backup procedures shall be implemented.		
5.4.1 System and application documentation are maintained at the off-site storage location.	1. Interview persons at the primary site who are responsible for storing documents off-site. 2. Review documentation supporting maintenance of the required off-site storage. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-2.1.2 NIST 800-26 9.2.7
Guidance: Current systems and applications documentation should be available off-site in case the primary processing site is disabled. Related CSRs: 5.7.3		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.4.2 Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent operation of the required rotation. 3. Verify by inspection the location of specific backup files. 4. Review documentation confirming successful periodic test of the ability to recover using backup files.	FISCAM TSC-2.1.1 HIPAA 164.308(a)(7)(ii)(B) NIST 800-26 9.2.6
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. Related CSRs: 5.11.1, 5.9.8, 5.4.6		
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

5.4.3 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.

1. By inspection, verify that the backup storage and alternate processing sites are consistent with available documentation.
2. Review documentation confirming that the backup storage and alternate processing sites meet the stated requirements.

FISCAM TSC-2.1.3
NIST 800-26 9.2.5
NIST 800-26 9.2.9

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.

Related CSRs: 5.11.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.4.4 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.

1. Observe the initiation of delivery of critical data from the primary site to the off-site facility.
2. Review the Contingency Plan to verify that it contains the specified elements.
3. Review records of data backups.

HIPAA 164.310(d)(1)
CMS Directed
HIPAA 164.308(a)(7)(ii)(A)
NIST 800-26 9.1.1

Guidance: Refer to Appendix B of the BPSSM.

Related CSRs: 5.11.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.4.5 A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.

An inventory of all equipment and software should be maintained, including the location and person responsible.

HIPAA 164.310(d)(2)(iv)

Guidance: A record should be use to track the movement all resources.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 logged with name, date, time, and action.

1. Review backup logs.
2. Inspect off-site backups.

ARS 9.9

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.

Related CSRs: 5.4.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.

FISCAM TSC-1.3
HIPAA 164.308(a)(7)(ii)(C)

Guidance: Processing priorities should exist for all critical functions and processes to be accomplished during an emergency. These should be periodically reviewed for accuracy.

Related CSRs: 5.3.1, 5.6.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.

1. Interview a sample of employees to confirm their understanding of their roles in emergency response procedures.
2. Review training records to confirm required training has been conducted, and is consistent with the current procedures.
3. Review training plans for future training in emergency actions.

FISCAM TSC-2.3.1
ARS 4.1
NIST 800-26 9.3.2

Guidance: There should be evidence that the employees have periodically received training relative to what to do in an emergency.

Related CSRs: 1.1.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.6.2 Emergency procedures are documented.	By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan.	FISCAM TSC-2.3.3 HIPAA 164.308(a)(7)(i) HIPAA 164.308(a)(7)(ii)(C)
Guidance: Procedures for use in an emergency should exist for automated and manual processes. They should be readily available. Refer to Appendix B of the BPSSM.		Related CSRs: 1.1.7, 2.2.14, 2.4.1, 3.5.6, 4.1.3, 5.2.7, 6.1.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.6.3 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.	1. Review training records to confirm that the required training has been delivered periodically. 2. Review training plans for future training in emergency actions.	FISCAM TSC-2.3.2
Guidance: These are procedures primarily for staff and management working in a data processing center environment.		Related CSRs: 1.1.7, 5.1.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.6.4 Emergency procedures are periodically tested.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming completion of the required testing. 3. Review future test plans to ensure that the emergency procedures are scheduled to be properly tested. 4. Interview data center staff.	FISCAM TSC-2.3.4 HIPAA 164.308(a)(7)(ii)(D)
Guidance: 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.		Related CSRs: 5.2.7, 5.5.1, 5.7.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.7 The contingency plan shall be annually reviewed and tested.		
5.7.1 The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.	1. Review documentation of annual conduct of the required test. 2. Review documentation describing how the testing conditions simulate an emergency or disaster. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review test plans for upcoming contingency plan testing, including lessons learned from the previous testing.	FISCAM TSC-4.1 CMS Directed HIPAA 164.308(a)(7)(ii)(D) ARS 5.4 ARS 5.5 NIST 800-26 4.1.4 NIST 800-26 9.3
Guidance: It is advisable to conduct "live tests" of critical system processes to ensure they will function in an emergency.		Related CSRs: 5.6.4, 2.5.9
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.7.2 Contingency Plans and associated documentation are reviewed and, if required, updated whenever new operations are planned or new safeguards contemplated.	1. Review the current Contingency Plan to confirm it is updated as required. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-3.1.1 CMS Directed ARS 5.4 ARS 5.5 NIST 800-26 9.2 NIST 800-26 10.2.12
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.		Related CSRs: 1.9.5, 1.12.2, 3.5.6, 6.3.10, 5.2.8
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent annual review, reassessment, and appropriate revision of the contingency plan as specified. 3. Review documentation confirming the required off-site distribution and storage.	FISCAM TSC-3.1.4 FISCAM TSC-3.1.1 FISCAM TSC-3.1.5 CMS Directed NIST 800-26 9.2.10 NIST 800-26 9.3.1

Guidance: Current contingency plans should be readily available to key persons during an emergency. Off-site storage will help ensure this availability. Related CSRs: 5.4.1, 5.9.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.7.4 Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review distribution records or interview senior management to ensure that they received the latest contingency plan test results and lessons learned information.	FISCAM TSC-4.2.1

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. Related CSRs: 3.5.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documents establishing that the contingency plan and related agreements are adjusted as specified.	FISCAM TSC-4.2.2 HIPAA 164.308(a)(7)(ii)(D) NIST 800-26 9.3.3

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.8 Resources supporting critical operations shall be identified.

5.8.1 Resources supporting critical and sensitive operations are identified and documented. Types of 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documents identifying resources supporting critical and sensitive operations for inclusion of the specified resource types.	FISCAM TSC-1.2 NIST 800-26 9.1 NIST 800-26 9.1.2

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. Related CSRs: 5.3.1, 2.1.3, 5.4.4, 5.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Service Continuity*

General Requirement Control Technique	Protocol	Reference
5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.		
5.9.1 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.	1. Interview users. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review the performance records to ensure the goals are clearly stated in writing.	FISCAM TSC-2.4.9
Guidance: To avoid a break in continuity of service, hardware performance should be evaluated frequently and users polled relative to level of service provided.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.2 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of the required logs. 3. Review documentation supporting conduct of the required analyses.	FISCAM TSC-2.4.8
Guidance: Hardware problems should be carefully analyzed in order to determine the maintenance needs and to prevent major failures.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.3 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.	FISCAM TSC-2.4.10
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.		Related CSRs: 1.9.1, 5.7.3, 6.3.4, 10.7.3, 6.6.1, 3.4.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.4 Goals are established by senior management for the availability of data processing and on-line services.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming establishment of the required goals.	FISCAM TSC-2.4.6
Guidance: Reasonable data processing goals should be set by management to guide the maintenance and problem analysis relative to hardware performance and availability.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.5 Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	1. Review records of past advanced notifications. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.	FISCAM TSC-2.4.11
Guidance: Notice of at least 2 days should be given to users relative to hardware changes.		Related CSRs: 5.7.3, 10.7.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Service Continuity*

	General Requirement / Control Technique	Protocol	Reference
5.9.6	Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.	FISCAM TSC-2.4.4
	Guidance: The operational flow of business functions should be designed to permit unscheduled interruptions without adversely affecting critical processes and deliveries.		Related CSRs: 2.2.24
	☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.7	Records are maintained on the actual hardware performance in meeting service schedules.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the required records.	FISCAM TSC-2.4.7
	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.		Related CSRs:
	☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.8	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	1. Review documentation confirming availability of spare or backup hardware for support of applications designated as critical or sensitive. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review operations and maintenance documentation to confirm that levels of available backup or spare hardware have been sufficient to support system availability objectives.	FISCAM TSC-2.4.5
	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.		Related CSRs: 5.4.2, 5.4.3, 5.10.1, 5.11.1, 5.11.2
	☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
5.9.9	Hardware maintenance policies and procedures exist and are up-to-date.	1. Inspect maintenance policies and procedures. 2. Review documentation supporting the contention that the required policies and procedures are up-to-date. 3. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	FISCAM TSC-2.4.1
	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.		Related CSRs: 1.9.1, 1.4.1, 1.8.4
	☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

General Requirement / Control Technique	Protocol	Reference
5.9.10 Regular and unscheduled hardware maintenance performed is documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance documentation for conformance with the documented procedures.	FISCAM TSC-2.4.3

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.

Related CSRs: 1.8.4, 1.9.5

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.9.11 Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	1. Inspect hardware maintenance schedules 2. Review documentation supporting the contention that the hardware maintenance schedule complies with vendor specifications. 3. Review maintenance records to confirm completion of hardware maintenance in accordance with the schedule. 4. Review documentation supporting the contention that the manner of performing maintenance minimizes the impact of maintenance on operations.	FISCAM TSC-2.4.2 NIST 800-26 7.1.14

Guidance: Maintenance schedules should be distributed and kept at different locations in the enterprise.

Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review documentation supporting the contention that alternate facilities have sufficient processing capacity. 2. Inspect agreements established to confirm coverage of all identified alternate facilities. 3. Review documentation identifying facilities required for alternate data processing and telecommunications. 4. Review documentation supporting the contention that alternate facilities are in the required state of readiness. 5. Review documentation supporting the contention that alternate facilities are available for use.	FISCAM TSC-3.2.1 CMS Directed NIST 800-26 9.2.4

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.

Related CSRs: 2.2.27, 5.1.7, 5.4.2, 5.4.3, 5.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.10.2 Alternate telecommunication services have been arranged.	Review documentation confirming the arrangement of alternate telecommunication services.	FISCAM TSC-3.2.2

Guidance: A careful analysis should be made of all telecommunications utilized in normal times, and the links necessary to support critical functions identified.

Related CSRs: 5.7.5, 5.8.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

General Requirement / Control Technique	Protocol	Reference
5.10.3 Arrangements are planned for travel and lodging of necessary personnel, if needed.	Verify by inspection that the required arrangements have been planned.	CMS Directed FISCAM TSC-3.2.3

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the required contingency plan(s) to confirm inclusion of the specification of storage location(s) for backup data and software. 2. Review documentation confirming that the specified plan is available for each standalone workstation.	CMS Directed

Guidance: Standalone workstations must be protected and contingency plans made for backup of their resident software and data.

Related CSRs: 5.4.2, 1.13.1, 1.13.5, 2.2.12, 7.4.2, 5.4.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.11.2 Standalone computer workstation backup data, software and current operating procedures are stored in accordance with the Contingency Plan.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Through inspection for a sample of standalone workstations, establish that the specified storage criteria are met.	CMS Directed

Guidance: It is suggested that this back-up information be stored at a location different from the workstations.

Related CSRs: 5.2.9, 5.4.3, 5.4.2, 5.9.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

5.12 Detection of malicious software shall be performed.

5.12.1 The CMS Business Partner shall use special software to accomplish malicious software identification, detection, protection, and elimination.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the required software is installed and operational in accordance with documented policy.	FISCAM TCC-1.3.2 HIPAA 164.308(a)(5)(ii)(B)

Guidance: This special software should be approved and tested by knowledgeable persons before being installed.

Related CSRs: 1.1.1, 1.9.1, 2.2.24, 10.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the documented procedure required to process emergency changes. 2. Interview the operations supervisor, computer operations management, programming supervisors, and user management. 3. For a sample of emergency changes, observe the required documentation and approval steps. 4. Review test plans and reports for the emergency changes.	FISCAM TCC-2.2.2 NIST 800-26 10.2.11

Guidance: Ensure that the emergency software changes are subsequently tested.

Related CSRs: 6.3.2, 6.6.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: ***Application Software Development and Change Control***

General Requirement Control Technique	Protocol	Reference
6.1.2 Emergency change procedures are documented.	Review the documentation of emergency change procedures.	FISCAM TCC-2.2.1

Guidance: Ensure that the procedures for making emergency software changes are current. Related CSRs: 1.1.7, 2.4.1, 2.4.2, 3.5.6, 5.6.2, 1.9.3, 10.7.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the required policies, and verify that they are enforced. 2. Interview the security administrator.. 3. Interview users.	FISCAM TCC-1.3.1

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. Related CSRs: 1.13.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.1 Test plans are documented and approved that define responsibilities for each party involved.	1. Interview test manager, and others as deemed necessary. 2. Interview the system manager. 3. Verify that test plans are documented and approved, and define the required responsibilities.	FISCAM TCC-2.1.4

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. Related CSRs: 2.5.11

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.3.2 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.	1. 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. 2. Review test plan to ensure that it addresses test levels and conditions.	FISCAM TCC-2.1.5

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. Related CSRs: 2.5.10, 2.5.11, 3.5.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

6.3.3 A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live test data are not to be used in testing.	1. Confirm the restrictions in the use of live data. 2. Interview test programmers. 3. Interview the system manager. 4. Verify that test data will meet all processing criteria.	FISCAM TCC-2.1.6 FISCAM TCC-2.1.7 ARS 9.8 NIST 800-26 10.2.5

Guidance: 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. Related CSRs: 1.9.1, 2.5.10, 2.5.11, 3.5.1, 4.7.6, 5.9.3, 6.4.4, 9.8.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application Software Development and Change Control*

General Requirement / Control Technique	Protocol	Reference
6.3.4 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.	1. Review documentation of all required departments for prompt and accurate updating. 2. Interview the system manager. 3. Interview the document control person (librarian).	FISCAM TCC-2.1.10 NIST 800-26 3.2.4
Guidance: Documentation used by hardware, software, operations, and systems persons should reflect the latest system and software environment.		Related CSRs: 1.9.1, 1.9.7, 2.5.1, 2.5.10, 3.4.6, 5.4.1, 5.8.1, 6.5.1, 5.9.3, 1.9.3, 10.7.3, 1.2.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.5 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.	1. Interview the software programming supervisor. 2. Review documented software changes to verify the tracing process.	FISCAM TCC-2.1.3
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.		Related CSRs: 2.11.2, 2.11.4, 3.5.6, 6.1.1, 6.6.1, 10.7.3, 6.7.2, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.6 Program changes are controlled as they progress through testing and are moved into production only upon documented approval from users and system development management.	1. Interview user management. 2. Verify the documented approval of program changes before production implementation. 3. Interview system development management.	FISCAM TCC-2.1.9 NIST 800-26 3.2
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.		Related CSRs: 3.4.5, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.7 Test results are reviewed and documented.	1. Verify that test results are reviewed and documented. 2. Interview the system manager.	FISCAM TCC-2.1.8 NIST 800-26 3.2.2
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.		Related CSRs: 2.5.10
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.8 Changes to detailed system specifications are prepared by the programmer and reviewed by the appropriate supervisor or manager.	1. Interview the programming supervisor. 2. Review documented changes to system specifications.	FISCAM TCC-2.1.2 NIST 800-26 10.2.4
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.9 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).	1. Ensure through observation or interviews that during testing persons/groups fulfilled their responsibilities. 2. Review test plan standards, and confirm that they follow all levels of testing and responsibilities. 3. Interview department supervisors to verify their compliance with test plan standards.	FISCAM TCC-2.1.1
Guidance: A good practice is to have independent tests performed.		Related CSRs: 1.4.4, 2.5.11
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application Software Development and Change Control*

General Requirement Control Technique	Protocol	Reference
6.3.10 Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	1. Interview the system programmers and/or system administrator. 2. Determine when the last production program change was reviewed, and how often. 3. Interview data center management and/or the security administrator.	FISCAM TCC-2.1.11
Guidance: Access controls and change controls should be periodically reviewed and/or tested to ensure their proper function.		Related CSRs: 3.1.2, 3.1.3, 3.3.3, 3.4.1, 4.4.1, 7.3.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.11 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 Roadmap.	1. Interview the system manager. 2. Confirm that the SDLC includes the four required elements.	FISCAM TCC-1.1.1 ARS 3.14 ARS 4.1 NIST 800-26 3.1 NIST 800-26 3.2.1 NIST 800-26 3.1.6
Guidance: Ensure that a current SDLC methodology exists, addresses security has been reviewed, and is being followed.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.12 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.	1. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current. 2. Examine training plans and records. 3. Interview the programming staff and the software staff.	FISCAM TCC-1.1.2 ARS 4.3
Guidance: Training plans and materials should exist for training in SDLC methodology.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.13 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.	1. Interview system programmers and administrators. 2. Interview the application system managers. 3. Review the documented policy to ensure that the required responsibilities are assigned.	CMS Directed HIPAA 164.310(a)(1) ARS 5.1 ARS 10.8
Guidance: Tests should be performed and test reports should be reviewed to ensure that safeguards that protect software from unauthorized modification have been tested.`		Related CSRs: 1.5.2, 1.5.6, 1.9.5, 5.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.3.14 Immediate (as required functionality allows) installation of vendor-supplied service packs, hotfixes, 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 protect system assets.	1. Review system configuration logs. 2. Review configuration management logs/procedures. 3. Review change approval policies and procedures. 4. Determine if any security fix has not been implemented and time of availability.	ARS 7.17 NIST 800-26 11.1.1
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.		Related CSRs: 1.9.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application Software Development and Change Control*

General Requirement / Control Technique	Protocol	Reference
6.4 Access to program libraries shall be restricted.		
6.4.1 Access to all programs, including production code, source code, and extra program copies, is protected by access control software and operating system features.	1. For critical software production programs, determine whether access control software rules are clearly defined. 2. Determine if the access controls are implemented and working.	HIPAA 164.312(e)(1) FISCAM TCC-3.2.3 HIPAA 164.312(a)(1)
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.		Related CSRs: 5.2.9, 1.4.4, 1.5.6, 2.8.6, 3.3.1, 10.10.1, 2.10.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.4.2 All deposits and withdrawals of program tapes and other storage media to/from the library are authorized and logged.	1. Select other storage media from the log 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 log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tape.	FISCAM TCC-3.2.4 NIST 800-26 7.1.3 NIST 800-26 10.1.2
Guidance: The library log should be protected from exposure to unauthorized changes or release.		Related CSRs: 1.3.12, 2.2.8, 2.2.23, 2.8.6
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.4.3 Production source code is maintained in a separate archive library.	1. Monitor libraries in use. 2. 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.	FISCAM TCC-3.2.2
Guidance: The separate archive library should be protected from unauthorized access by software or physical controls.		Related CSRs: 2.10.2
☑ *SS* ☑ *PSC* ☐ *PartB* ☑ *PartA* ☐ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
6.4.4 Separate libraries are maintained for program development and maintenance, testing, and production programs.	1. Interview library control personnel. 2. Monitor libraries in use.	FISCAM TCC-3.2.1
Guidance: The separate libraries should each have their own set of access controls so that, for example, testers cannot access production code.		Related CSRs: 2.10.2, 3.4.5, 6.8.2, 2.2.29
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.5 Distribution and implementation of new or revised software shall be controlled.		
6.5.1 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.	1. Examine distribution and implementation procedures for distributing new or revised software. 2. Check the distribution and implementation orders for a sample of changes.	FISCAM TCC-2.3.2 NIST 800-26 10.2.7 NIST 800-26 10.2.10
Guidance: The implementation order should leave no doubt as to when the new software should start to be used for production.		Related CSRs: 1.9.5, 3.5.1, 6.3.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.5.2 Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.	FISCAM TCC-2.3.1
Guidance: Software should be distributed allowing enough time at the site for installation, testing, and migration to production.		Related CSRs: 1.9.1, 2.11.2, 3.1.3, 3.4.1, 3.4.4, 3.5.4, 10.7.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Application Software Development and Change Control***

General Requirement Control Technique	Protocol	Reference
6.6 Programs shall be automatically labeled and inventoried.		
6.6.1 Library management software is used to produce audit trails/logs 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.	1. Interview personnel responsible for library control. 2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures. 3. Review software change control policies and procedures.	FISCAM TCC-3.1 ARS 11.2 ARS 11.3 NIST 800-26 10.2.8
Guidance: Software controls should be easily monitored and audited. Library management of software helps ensure that differing versions are not accidentally misidentified.		Related CSRs: 6.3.5, 2.11.2, 2.11.4, 3.5.4, 3.5.6, 5.9.3, 6.1.1, 6.3.5, 10.7.3, 10.10.1, 6.8.2, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.7 Authorizations for software modifications shall be documented and maintained.		
6.7.1 Change requests are approved by both system users and data processing staff.	1. Determine if the change requests for past changes have been approved. 2. Interview software development staff. 3. Identify recent software modifications and determine whether change request forms were used.	FISCAM TCC-1.2.2
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.		Related CSRs: 3.5.4, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.7.2 Software change request forms are used to document software modification requests and related approvals.	Examine a selection of software change or modification request forms for approvals.	FISCAM TCC-1.2.1 NIST 800-26 3.1.4 NIST 800-26 10.2.3
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.		Related CSRs: 3.3.4, 6.3.5
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.8 Movement of programs and data among libraries shall be controlled.		
6.8.1 Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.	1. Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared. 2. Examine some of the images of stored code that has been changed.	FISCAM TCC-3.3.2
Guidance: An independent library control group should make the image comparisons.		Related CSRs: 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
6.8.2 A group independent of the user and programmers controls movement of programs and data among libraries.	Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.	FISCAM TCC-3.3.1
Guidance: Prior to moving software from a test to production environment, an independent review of the changes developed and tested should be made.		Related CSRs: 2.10.2, 3.4.2, 6.3.9, 6.4.2, 6.4.4, 6.6.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application System Authorization Controls*

General Requirement / Control Technique	Protocol	Reference

7. *Application System Authorization Controls*

7.1 Source documents shall be controlled and shall require authorizing signatures.

7.1.1	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.	1. Review the documented procedure for batch control sheet preparation. 2. Check a sample of batch control sheets to ensure the inclusion of the Control Technique elements.	FISCAM TAN-1.1.4

Guidance: A preformatted batch control sheet will simplify the tracking process for batch application systems or interactive systems with batching capabilities. Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

7.1.2	Access to blank documents (checks, claims forms, etc.) is restricted to authorized personnel.	1. Interview a sample of personnel to confirm use of documented handling procedures. 2. Inspect blank document storage access controls for conformance to documented policy. 3. Review documented procedure containing authorized names and control of access.	FISCAM TAN-1.1.1

Guidance: It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents. Related CSRs: 1.1.8

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

7.1.3	Source documents (checks, claims forms, etc.) are pre-numbered to maintain control over the documents. Key source documents require authorizing signatures.	1. Inspect audit data confirming that the required process is consistently used. 2. Confirm that documents contain authorized signatures. 3. Review the documented procedure for recording and tracking of document numbers. 4. Review documentation identifying "key source documents".	FISCAM TAN-1.1.2 FISCAM TAN-1.1.3

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. Related CSRs: 2.6.1, 2.13.1

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.	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.	FISCAM TAN-3.1.1

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. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application System Authorization Controls*

General Requirement / Control Technique	Protocol	Reference
7.2.2 Master files and program code that does the verification are protected from unauthorized modification.	1. Identify and observe the procedures employed that protect master files and program code. 2. Review the documented procedure covering the protection of master files and program code. 3. Inspect audit data confirming that the required process is consistently used. 4. Review documentation of software controls used in providing the required protection.	FISCAM TAN-3.1.2

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.

Related CSRs: 5.2.9, 2.6.1, 2.13.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

7.3 Data entry workstations shall be secured and restricted to authorized users.

7.3.1 All transactions are logged as entered, along with the User ID of the person entering the data.	1. Observe the processing of sample transactions, to ascertain that they are being logged correctly. 2. Review the documented procedure prescribing transaction logging.	FISCAM TAN-2.1.9

Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the data entry process is correct.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

7.3.2 Each operator is required to use a unique password and identification code before being granted access to the system.	1. 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. 2. Review documented login procedure. 3. Observe a sample of data entry login.	FISCAM TAN-2.1.4

Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses, including the use of password and identification control.

Related CSRs: 2.9.10

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

7.3.3 When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	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. Observe physical area during non-business hours.	FISCAM TAN-2.1.2

Guidance: Review the workstation policy/guidelines.

Related CSRs: 1.13.1, 2.2.12

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

7.3.4 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.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation use. 3. Observe workstation use.	FISCAM TAN-2.1.5

Guidance: Review the workstation policy/guidelines.

Related CSRs: 1.13.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application System Authorization Controls*

General Requirement Control Technique	Protocol	Reference
7.3.5 Each workstation automatically disconnects from the system when not used after a specific period of time.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation configuration and use. 3. For a sample of workstation types, observe operation of the automatic disconnect process.	CMS Directed FISCAM TAN-2.1.6 ARS 7.15 ARS 7.16 NIST 800-26 16.2.6
Guidance: Review the workstation policy/guidelines. Additionally, it is a good practice to review the audit logs to validate the workstation disconnect functionality.		Related CSRs: 1.13.1, 2.6.1, 2.13.1, 2.9.11, 2.9.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.6 Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.	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.	FISCAM TAN-2.1.8 NIST 800-26 16.1.1
Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the online access process is correct.		Related CSRs: 6.3.10, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1, 2.9.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.3.7 Data entry workstations are located in physically secure environments and monitors are positioned to eliminate viewing by unauthorized persons.	1. Review System Security Plan. 2. Observe the location of workstations and their monitors.	FISCAM TAN-2.1.1 NIST 800-26 7.2.1
Guidance: Workstations processing or connected to systems processing sensitive data are located in physically secure areas.		Related CSRs: 2.2.12
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*		
7.4 Users shall be limited to a set of authorized transactions.		
7.4.1 Authorization profiles for users limit what transactions data entry personnel can enter.	1. Review audit controls used to assure continued application of the required procedure. 2. Review documented procedure for data entry to confirm enforcement of the required limitation.	FISCAM TAN-2.2.2
Guidance: Review the application processing policy/guidelines.		Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.4.2 Authorization profiles for users or workstations limit what transactions can be entered.	1. 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. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of configuration management assuring continued operation of the required controls. 4. Review documents designating transactions authorized from each workstation.	FISCAM TAN-2.2.1
Guidance: The supervisors should address limitations in access for inclusion in the ACL.		Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Application System Authorization Controls*

General Requirement Control Technique	Protocol	Reference
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.	1. Inspect audit data confirming that the required process is consistently used. 2. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.	FISCAM TAN-3.2.1
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.		Related CSRs: 1.13.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.6 Independent reviews of data shall occur before entering the application system.		
7.6.1 Procedures are in place for a multilevel review of CMS sensitive input data before it is released for processing.	1. Review documented procedure for pre-processing of data. 2. Interview a sample of supervisors and control unit personnel to confirm use of the process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAN-1.2.3
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
7.6.2 Data control unit personnel monitor data entry and processing of source documents.	1. Interview management and data control unit personnel to confirm use of the process. 2. Review documented data entry and processing procedures. 3. Observe data entry and processing procedures.	FISCAM TAN-1.2.2
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.		Related CSRs: 8.4.5, 8.5.1, 8.5.2
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
7.6.3 Data control unit personnel verify that source documents are properly prepared and authorized.	1. Inspect audit data confirming that the required process is consistently used. 2. Interview management and data control unit personnel to confirm use of the process. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Observe data control unit personnel performing the verification process.	FISCAM TAN-1.2.1
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.		Related CSRs: 8.4.5, 8.5.1, 8.5.2
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		

Category: *Application System Completeness Controls*

General Requirement / Control Technique	Protocol	Reference

8. *Application System Completeness Controls*

8.1 Computer sequence-checking shall be implemented.

8.1.1	Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review reports of missing or duplicate transactions. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.2.4

Guidance: 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.

Related CSRs: 7.3.1, 7.3.6, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

8.1.2	Sequence checking is used to identify missing or duplicate transactions.	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.	FISCAM TCP-1.2.3

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. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4, 8.2.1

☑ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

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.	1. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers. 2. Review the documented procedure that prescribes the assigning of unique sequence numbers. 3. Inspect audit data confirming that the required process is consistently used. 4. 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. 5. Interview the system owner and determine what policies and corrective action are in place when a sequence number error occurs.	FISCAM TCP-1.2.2

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.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application System Completeness Controls*

General Requirement / Control Technique	Protocol	Reference
8.1.4 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.	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.	FISCAM TCP-1.2.1

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.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.	1. Verify the application has an assigned system owner. 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. 4. Verify the application has the ability to insert the preassigned source document numbers matched with the associated data.	FISCAM TCP-1.3.2

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.

Related CSRs: 7.3.1, 7.3.6, 8.1.2, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.	1. Verify that a system owner has been designated and when errors occur, that person is notified. 2. Review the program specifications that describe the computer matching process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.3.1

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.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4, 9.3.5, 9.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the documented procedure that describes the comparison process. 2. Verify that a staff person is assigned and responsible for verifying that high-value transaction data accurately reflects data from the source documentation. 3. Inspect documentation identifying items designated as high-value, low volume. 4. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.4

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.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

Category: ***Application System Completeness Controls***

General Requirement Control Technique	Protocol	Reference
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.	1. Inspect audit data confirming that the required process is consistently used. 2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application. 3. Review the documented procedure describing the reconciliation process.	FISCAM TCP-2.2 NIST 800-26 11.2.1
Guidance: This process is application dependent, but should be automated as much as possible.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review the documented procedures for the data entry process. 2. Review a sample of data control reports for completeness of data entry. 3. This process is application dependent, but should be automated as much as possible. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.	FISCAM TCP-2.1.1
Guidance: The application should be tracking each transaction and reconciling any differences with the data being entered. (commonly called "run-to-run control totals")		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Verify that the application contains routines for process checking. The checking process should be included in applicable trailer labels. 2. Interview the supervisory application programmer to determine that system controls are in place as prescribed by the application programs. 3. Inspect audit data confirming that the required process is consistently used. 4. Review the program specifications describing the reconciliation process for accurate data entry.	FISCAM TCP-2.1.2
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Application System Completeness Controls***

General Requirement / Control Technique	Protocol	Reference
8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	1. Review the documented procedures describing the reconciliation process for data entry. 2. Interview the supervisory application programmer to determine implementation of automatic reconciliation in completion of computer job runs. 3. Inspect audit data confirming that the required process is consistently used. 4. Verify bends and processing errors are reconciled between the completion of one job and before the start of the next job. The reconciliation process should not stop all batch processing.	FISCAM TCP-2.1.3
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
8.4.4 System interfaces require that the sending system's output control counts equal the receiving system's input counts.	1. Review the documented procedure describing the reconciliation process between systems. 2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-2.1.4
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
8.4.5 A data processing control group receives and reviews control total reports and determines the completeness of processing.	1. Review the documented procedure describing the data control group's function. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-2.1.5
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3
☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedures for the data control and data entry process for inclusion of the required process.	FISCAM TCP-1.1.2
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.		Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		

Category: ***Application System Completeness Controls***

General Requirement Control Technique	Protocol	Reference
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.	1. Inspect the process and documents for developing record counts and control totals to determine data entry completeness. 2. Review the documented procedures for the data control process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.1.1

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.

Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

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 Errors are corrected by the user originating the transaction.	1. Interview a sample of supervisors and subordinate personnel to confirm use of the documented procedure. 2. Inspect audit data confirming that the required process is consistently used. 3. Review the documented error correction procedure.	FISCAM TAY-3.2.2

Guidance: 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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

9.1.2 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.	1. Interview a sample of supervisors and subordinate personnel to confirm that all specified reports and files have the required characteristics.. 2. Review sample error reports/files, and confirm that error messages contain the information specified in the Control Techniques. 3. Review the documented error processing procedure.	FISCAM TAY-3.2.1

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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.1.3 All corrections are reviewed and approved by supervisors before the corrections are reentered. (Based on Medicare operating environment CMS Business Partners may have other compensating controls in place.)	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented error correction procedure for inclusion of the required process. 3. Interview a sample of supervisors and subordinate personnel to confirm use of the required process.	FISCAM TAY-3.2.3

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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference

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.

Protocol: Review the documentation explaining how the specified objective is met.

Reference: FISCAM TAY-1.4

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.

Related CSRs: 2.2.16

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.

Protocol:
1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented procedure for processing reject data to confirm inclusion of the specified features.

Reference: FISCAM TAY-3.1.1

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.

Related CSRs: 9.1.2, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.1, 9.3.6, 9.7.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.3.2 A control group is responsible for controlling and monitoring rejected transactions.

Protocol:
1. Review the documented procedure describing the control group's responsibilities and duties.
2. Interview a sample of the control group to confirm operational responsibilities match those documented.

Reference: FISCAM TAY-3.1.3

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.

Related CSRs:

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

9.3.3 General controls effectively protect the suspense file from unauthorized access and modification.

Protocol: Review the documentation describing how general controls provide the required protection of the suspense file.

Reference: FISCAM TAY-3.1.6

Guidance: 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.

Related CSRs: 5.2.9, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

9.3.4 The suspense file is purged of transactions as they are corrected.

Protocol:
1. Review the documented procedure for the error correction process to confirm inclusion of the specified process.
2. Inspect audit data confirming that the required process is consistently used.

Reference: FISCAM TAY-3.1.4

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.

Related CSRs: 2.8.2

☑ *SS* ☑ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference
9.3.5 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.	1. Review the documented procedure for suspense file processing and transaction reconciliation. 2. Observe the suspense file process to confirm that the documented procedure is followed. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-3.1.2

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.

Related CSRs: 8.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☑ *CWF* ☑ *COB*

9.3.6 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.	1. Review the documented suspense file procedure for inclusion of the specified processes. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-3.1.5

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.

Related CSRs: 9.1.2, 9.3.1, 8.2.2, 9.5.1, 9.6.7, 9.6.8, 3.1.5

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☐ *DC* ☐ *CWF* ☑ *COB*

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.	1. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry". 2. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.	FISCAM TAY-1.1.1 FISCAM TAY-1.1.2

Guidance: A good approach is to have needed data entry information succinctly formatted to facilitate ease of data entry.

Related CSRs: 1.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 logged by the application so that the action can be analyzed for appropriateness and correctness.	1. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-2.3.1 FISCAM TAY-2.3.2

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.

Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

Category: ***Application System Accuracy Controls***

General Requirement / Control Technique	Protocol	Reference

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.

1. Review the documented procedure assigning responsibility for output production and distribution.
2. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.

Reference: FISCAM TAY-4.1.1

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.

Related CSRs: 1.4.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming use of the required process.
3. Review documentation describing how the required control is implemented.

Reference: FISCAM TAY-4.1.6

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.

Related CSRs: 9.8.1, 9.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.6.3 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.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect the required schedule to confirm inclusion of the required elements.
3. Inspect audit data confirming that the required process is consistently used.

Reference: FISCAM TAY-4.1.2

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.

Related CSRs: 1.5.2, 1.5.5

☐ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.6.4 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review sample printed reports to verify that it contains the elements required in the Control Technique.

Reference: FISCAM TAY-4.1.3

Guidance: The printed report name, time, and date are good management tools to assist in the tracking of completed tasks.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.6.5 Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review logs and check sample output, to verify that the required information is recorded.

Reference: FISCAM TAY-4.1.4
NIST 800-26 8.2.3

Guidance: The output report log is a good management tool to assist in the tracking of completed tasks.

Related CSRs: 1.5.2, 3.2.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Application System Accuracy Controls*

General Requirement / Control Technique	Protocol	Reference
9.6.6 Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure describing the output process and supervisory review.	FISCAM TAY-4.1.7

Guidance: The printed reports are good management tools to assist in the tracking of completed tasks. Related CSRs: 1.5.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.6.7 A control log of output product errors is maintained, including the corrective actions taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review the control log and confirm that it contains the required information.	FISCAM TAY-4.1.8

Guidance: The control log, 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. Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

9.6.8 Output from reruns is subjected to the same quality review as the original output.	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.	FISCAM TAY-4.1.9

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted. Related CSRs: 2.1.2, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review the documented procedure describing the review process and detailed report constituency. 2. Inspect audit data confirming that the required process is consistently used. 3. Review sample reports to confirm that they include the required elements specified in the Control Technique.	FISCAM TAY-4.2

Guidance: The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness. Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.4.1, 3.1.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

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.	1. Review the documented procedure describing the protection provided program code, files, or tables. 2. Observe the actions or procedures in place that protect program code, files, or tables.	FISCAM TAY-2.1.4 FISCAM TAY-2.2.1 FISCAM TAY-2.2.2 ARS 9.8

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. Related CSRs: 5.2.9, 9.6.2, 3.4.1

☑ *SS* ☑ *PSC* ☐ *PartB* ☑ *PartA* ☐ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*

Category: ***Application System Accuracy Controls***

General Requirement / Control Technique	Protocol	Reference
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.	1. Review the documented procedure describing programmed validation and edits for inclusion of the specifically required checks. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-2.1.1 ARS 9.8
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.		Related CSRs: 9.6.2, 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	1. Review the documented procedure describing the specified validation and editing process. 2. Inspect audit data confirming that the required process is consistently used. 3. Observe the validation and edit process.	FISCAM TAY-2.1.2 FISCAM TAY-2.1.3 ARS 9.8
Guidance: Validation of the accuracy of data assists in the integrity of the data being processed.		Related CSRs: 3.4.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☐ *CWF* ☑ *COB*		
9.8.4 Integrity verification programs are used by applications to look for evidence of data tampering, errors, and omissions.	Observe the actions or procedures in place that protect Medicare data.	NIST 800-26 11.2.4
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
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.	Observe the actions or procedures in place that protect Medicare data.	NIST 800-26 11.2
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.		Related CSRs:
☐ *SS* ☐ *PSC* ☐ *PartB* ☐ *PartA* ☐ *Dmerc* ☐ *DC* ☐ *CWF* ☐ *COB*		
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.	1. Review documented procedure specifying preformatted workstation screens, and describing screen prompts. 2. Observe a sample of workstation screens as personnel are processing data. 3. Interview the system administrator to confirm that the required feature is universally available..	FISCAM TAY-1.2
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.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement Control Technique	Protocol	Reference

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.

1. By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center.
2. Review audit data confirming control of access lists in accordance with documented procedures.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

CMS Directed

Guidance: Ensure that only personnel with a need-to-know have access to the list. Related CSRs: 2.2.23

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.1.2 Physical access to enclosures housing network equipment is restricted.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Select a sample of network equipment locations representative of the range of types of physical locations within each facility. For these sample equipment, confirm that access to them is restricted in accordance with the documented procedure.

CMS Directed

Guidance: Ensure that access to the area where the network equipment is located is controlled. Related CSRs: 2.2.15

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.2 Network system security shall be monitored for deficiencies.

10.2.1 Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation identifying devices selected to provide the specified logging function.
3. By inspection of a sample of the logs, confirm that they include network and system activity.

CMS Directed

Guidance: Ensure that logs are kept of network activity. Related CSRs: 10.2.4, 2.1.8

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.2.2 Real-time file scanning is enabled. Desktop virus scanning software is installed, real-time protection and monitoring is enabled, and the software is configured to perform full virus scans during system boot and every 12 hours. Virus-scanning software is provided at critical entry points, such as remote-access servers.

1. Confirm by inspection that virus-scanning software is installed.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation identifying designated critical network entry points.

CMS Directed
ARS 7.13
NIST 800-26 11.1
NIST 800-26 11.1.2

Guidance: A formal virus protection program should be established at the Network level. Related CSRs: 5.12.1, 10.7.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.2.3 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.	1. Review alarm and alert functions of any firewalls and other network perimeter access control systems to insure they are properly enabled. 2. Review operating system, user accounting, and application software audit logging processes on all host and server systems to insure they are properly enabled. 3. Review relevant policies and procedures for inclusion of the required process. 4. Review sample of intrusion detection audit logs for servers and hosts on the internal, protected, network.	CMS Directed ARS 10.1 NIST 800-26 11.2.5
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.		Related CSRs: 2.6.1, 10.2.5, 10.2.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.4 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.	1. Review network logs. 2. Interview technical staff. 3. Review IDS/Firewall logs. 4. Determine the method for alerts.	ARS 10.2
Guidance: Anomalies should be carefully analyzed to determine if unauthorized activity is occurring. Timely alerts are needed to initiate appropriate activities.		Related CSRs: 10.2.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.5 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 logged. Logs are retained for 90 days, and old logs are archived. Log archives are retained for one year.	1. Review router/firewall configuration. 2. Review router/firewall logs. 3. Determine expiration dates of appropriate logs.	ARS 11.4
Guidance: Ensure that logs from perimeter devices contain the required information, and that they are carefully reviewed on a frequent basis.		Related CSRs: 10.2.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.6 Stateful inspection and application firewall hardware and software are used.	1. Review firewall hardware and software configurations to determine compliance. 2. Utilize firewall reporting capabilities to review log on accounting, active connections, and effectiveness of alert settings.	ARS 6.1 NIST 800-26 16.2.11
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.		Related CSRs: 10.8.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.7 System logs 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.	1. Review alert notifications. 2. Interview technical staff	ARS 10.3 NIST 800-26 11.2.7
Guidance: Establish a policy to review system logs for the required events.		Related CSRs: 10.2.3, 10.9.1, 2.6.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.2.8 If keystroke monitoring is used, users are notified.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-26 17.1.9

Guidance: Establish a policy and procedures on the use and control of keystroke monitoring. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect logs confirming conduct of the required verification.	IRS 1075 5.8@8.2 CMS Directed

Guidance: A good approach might be a policy that requires verification of the receiving facsimile machine's telephone number. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 5.8@8.1 CMS Directed

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." Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.3 Controls exist to identify appropriate use of the E-mail system by employees, and to enforce E-mail authentication, security, privacy, and message integrity.	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-26 11.2.9

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Related CSRs: 10.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.4 Security policy exists and 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the audit process for operation in accordance with the documented process.	CMS Directed ARS 7.4

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. Related CSRs: 10.3.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.5 Fax procedures 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.	Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 5.8@8.3 CMS Directed

Guidance: Establish a formal procedure generating and attaching the required fax cover sheet. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.3.6 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 used, they must conform to FIPS 186-2.	Review relevant policies and procedures for inclusion and directed use of the required process.	ARS 8.2 NIST 800-26 15.1.2

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Related CSRs: 10.3.3, 10.3.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.4 Cryptographic tools shall be controlled.		
10.4.1 Sensitive information being electronically transmitted must be protected. Two acceptable methods for transmitting sensitive information over telecommunications devices: (1) encryption and (2) guided media.	1. Confirm by inspection that documented controls are in place and operational. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of controls used to assure protection of electronically transmitted sensitive information. 4. Review documentation establishing approval of the protection methods utilized.	HIPAA 164.312(e)(2)(ii) IRS 1075 5.8@1 FISCAM TAC-3.2.E.1 HIPAA 164.312(a)(2)(iv) ARS 9.2 NIST 800-26 16.2.14 NIST 800-26 7.2
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.		Related CSRs: 10.4.4, 10.4.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.4.2 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.	1. Review documentation establishing that the required protection has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.3 HIPAA 164.312(e)(2)(ii) HIPAA 164.312(a)(2)(iv)
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.		Related CSRs: 10.4.4, 10.4.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.4.3 The use of application security mechanisms, such as SSL and SSH, is both enabled and forced. Minimum encryption and password authentication are used in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).	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.	ARS 8.1
Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.		Related CSRs: 10.4.1, 10.4.2, 10.5.1, 10.8.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.4.4 Encryption protection is enabled for wireless media.	1. Review existing policies and procedures to ensure compliant encryption specified. 2. Perform testing to ensure encryption requirement met.	ARS 6.8 NIST 800-26 7.2
Guidance: Data sent via wireless media should be protected using encryption.		Related CSRs: 10.4.1, 10.4.2
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.4.5 If encryption is used, it must meet federal standards, and controls for key generation, distribution, storage, use, destruction, and archiving must be implemented.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-26 16.1.7 NIST 800-26 16.1.8
Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.5 Adequate Network password policies shall be implemented.		
10.5.1 Passwords are transmitted and stored using secure protocols and algorithms.	1. Review documentation of controls used to assure that all systems remain configured to use the specified feature. 2. Review documentation explaining how this feature is implemented on each network and local computing environment. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.7 FISCAM TAC-3.2.E.1 NIST 800-26 15.1.12
Guidance: Ensure that passwords are not transmitted as plain-text.		Related CSRs: 2.9.7, 10.10.1, 10.4.3
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6 Internet Security Policies shall be made available.		
10.6.1 CMS Business Partner's Internet connections must be in accordance with the CMS Internet Security Policy. 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. (See CMS Internet Security Policy, dated November 24, 1998).	1. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement. 2. 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. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. 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.	CMS Directed ARS 3.8 ARS 9.2 NIST 800-26 16.1.7
Guidance: At present, the internet may not be used for CMS sensitive data.		Related CSRs:
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6.2 Unless prior approval by CMS SSG is obtained, persistent cookies are prohibited.	1. Review software configuration logs/procedures. 2. If not currently in place, procedures to delete cookies should be developed and personnel trained on procedures.	ARS 8.3
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 log files and could also be used to track users browsing habits, cookies just make it easier.		Related CSRs: 1.13.1
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6.3 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.	Review web pages for compliance.	ARS 3.7 NIST 800-26 16.3.1
Guidance: Privacy policy banners should be displayed on Web pages where personal information is collected.		Related CSRs: 1.7.1, 2.8.7
☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: *Network*

General Requirement Control Technique	Protocol	Reference
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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing audit and inventory processes and tools in use to detect improper use of software.	CMS Directed
Guidance: A formal policy should be established regarding the use of purchased software. Related CSRs: 1.13.3		
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.7.2 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.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the specified controls are in place and operating in accordance with the documented procedure. 3. Review documentation describing the software tracking system implemented to provide the specified controls.	CMS Directed
Guidance: A formal program should be established with a policy and procedure. Related CSRs: 1.1.8, 6.5.2		
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.7.3 Change control is implemented to maintain control of changes to hardware, software, and security mechanisms.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming use of the documented change-control mechanism. 3. Review documentation describing the change-control mechanism that is implemented to provide the specified controls.. 4. For a sample of hardware, software, and security mechanism, determine by inspection that the configuration of the sample item matches the documented baseline configuration for the item. 5. Compare sampled data, such as device type, serial number, and software version, from the current configuration management baseline system description with corresponding hardware, software, and security mechanism implementation to confirm precise match.	CMS Directed
Guidance: A good approach might be to establish change control policies and procedures for all hardware, software, and security products. Related CSRs: 5.9.3, 6.6.1, 3.4.1, 1.9.3, 6.1.2, 6.3.4, 10.7.4		
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		
10.7.4 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.	1. Review logs. 2. Interview IT personnel.	ARS 10.4
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. Related CSRs: 10.7.3		
☑ SS ☑ PSC ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF ☑ COB		

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.7.5 All traffic for external communications is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.	Review packet screening rules.	ARS 6.2

Guidance: The packet screening rules should apply only to specified firewalls and routers. Related CSRs: 10.2.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 a gateway/firewall.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing controls implemented to insure compliance with this requirement.	IRS 1075 5.8@6 CMS Directed FISCAM TAC-3.2.E.1 NIST 800-26 16.2.10

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. Related CSRs: 10.8.5, 10.8.6, 1.13.6, 10.2.6

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.8.2	Authentication is used 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. Procedures for the above are documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of all required authentication functions.	HIPAA 164.312(d) CMS Directed ARS 1.1 ARS 1.5 ARS 7.1 ARS 7.11 NIST 800-26 16.2

Guidance: A formal program should be established with a policy and procedure. Related CSRs: 2.9.6, 2.9.5, 10.10.2, 10.10.3, 10.4.3

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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.	1. Review relevant policies and procedures for inclusion and directed use of the required process and specification of the warning message(s) to be used. 2. View the required warning message displayed on the opening screen seen by system users each type of server, workstation, and terminal used in the system. 3. For a sample, including each type of network device supporting the feature, view the required warning message displayed on the opening screen seen by anyone attempting to directly access the device from the network or console.	FISCAM TAC-3.2.E.2.1 ARS 3.6 NIST 800-26 16.2.13

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. Related CSRs: 2.8.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.8.4	Workstations with dial-up access generate a unique identifier code before connection is completed.	1. Review documented dial-up procedure to confirm inclusion of the required features. 2. Observe a sample of dial-up connections involving each type of access controller.	FISCAM TAN-2.1.7

Guidance: If workstations have dial-up access, ensure that a unique ID code is generated for each dial-up session. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.8.5 All servers allowing public access are placed within a DMZ, and direct access is not allowed to the internal network. DMZ servers cannot access the internal network. DMZ packet filtering and proxy rules provide protection for servers.	1. Review network diagrams for proper configuration in relation to 'CMS Internet Architecture document number CMS-CIO-STD-INT01'. 2. Review packet filtering/proxy rules.	ARS 6.6

Guidance: The architecture and the use of rules should prohibit unauthorized access to all servers. Related CSRs: 10.8.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.8.6 All network protocols not explicitly required for system and application functionality are disabled.	1. Examine network configuration logs for compliance. 2. Randomly review network protocols on desktop systems. 3. Review the policy/procedure.	ARS 7.10 NIST 800-26 16.2.2

Guidance: Develop and implement a way to verify that the protocols that are not required have been disabled. Related CSRs: 2.3.1, 10.8.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.9 Vulnerabilities to physical and cyber attacks shall be assessed.

10.9.1 A plan is in place to assess the risks to the network.	Review the required plan and approved implementing instructions.	PDD 63 333

Guidance: A formal program is in place for determining when and how to assess risks to the network. Related CSRs: 10.2.7

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.9.2 A plan is developed for eliminating significant vulnerabilities.	1. Review the required plan. 2. Review documentation establishing that the required plan eliminates all significant vulnerabilities.	PDD 63 338 NIST 800-26 10.3

Guidance: As part of the security management program, ensure that a plan is developed to minimize vulnerabilities. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.9.3 A plan is developed for alerting, containing, and rebuffing a physical or cyber attack on the CMS Business Partner IS systems.	Review the required plan to confirm that it includes the specified features.	PDD 63 350

Guidance: A formal program should be established with documented policies and procedures. Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.9.4 Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming conduct of the required assessments at least annually.	PDD 63 333 ARS 1.2

Guidance: As part of the security management program, ensure that an annual assessment is performed. Related CSRs: 1.9.8, 10.9.5

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.9.5 Penetration testing is performed as needed, and 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.	1. Review IOM summarizing the results of the penetration testing. 2. Interview SSO to determine findings and relevant documents.	ARS 10.7 NIST 800-26 1.1.5 NIST 800-26 2.1.4 NIST 800-26 10.3.1 NIST 800-26 10.3.2 NIST 800-26 11.2.8

Guidance: There should be documentation available showing that the penetration testing was accomplished according to appropriate standards and procedures. Related CSRs: 10.9.4

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

Category: *Network*

General Requirement / Control Technique	Protocol	Reference
10.9.6 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.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-26 14.2 NIST 800-26 14.2.1 NIST 800-26 14.2.2 NIST 800-26 14.2.3

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.

Related CSRs:

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

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 IDs 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 logs; (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.	1. Review documentation confirming implementation of communications software having all of the required features. 2. Review audit data confirming continuing operation of all specified features of the required software.	FISCAM TAC-3.2.E.1 ARS 7.15 ARS 7.21 NIST 800-26 7.2.2 NIST 800-26 16.2.1 NIST 800-26 16.2.8 NIST 800-26 16.2.9 NIST 800-26 16.2.15

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.

Related CSRs: 6.4.1, 2.9.6, 2.9.11, 2.8.4, 3.4.1, 2.9.8, 2.9.10, 3.6.2, 10.5.1

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.10.2	Remote access is enabled through VPN links, using authorized VPN client software. Encryption standards are used in combination with password authentication and certificate-based authentication or additional authentication protection (e.g., token-based, biometric).	1. Review remote access policies/procedures. 2. Check that remote access is implemented and controlled.	ARS 7.19

Guidance: Remote access should be controlled and there should be evidence of that control.

Related CSRs: 3.6.3, 10.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*

10.10.3	Secure management protocols are enabled through VPN link(s) if connected to a network, and Remote Administration is used. Encryption standards are used in combination with password authentication or additional authentication protection (e.g., token-based, biometric).	☐Review remote access policies/procedures.	ARS 7.20

Guidance: Remote administration should be carefully managed and controlled. Use of encryption features should be evaluated and approved by knowledgeable persons.

Related CSRs: 2.9.5, 10.8.2

☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*