DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security (IS) Guidebook for Audits

Version 1.0
March 31, 2005

EXECUTIVE SUMMARY AND INTRODUCTION

This guide has been developed to aid contractors in understanding and preparing for the various types of audits and reviews which may be performed at their locations.

This guide is meant to provide additional information on site selection criteria, audit steps and objectives, documentation requirements, the types of employees which will need to be interviewed, as well as space and equipment requirements for CFO audits, Section 912 Reviews, SAS 70 type II audits and Penetration/EVA testing.

I. CFO/EDP Audit Acts

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

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

II. Section 912 Evaluation

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

These evaluations are conducted according to procedures established by the Centers for Medicare & Medicaid Services, Office of Information Services (CMS) with input from the U.S. Department of Health and Human Services, Office of Inspector General (OIG). The procedures are organized using the eight FISMA statutory areas which include: Periodic risk assessments; Policies and procedures based on risk assessments that cost-effectively reduce risk to an acceptable level and ensure security is addressed within the Systems Development Life Cycle and complies with the National Institute of Standards and Technology standards; Systems security plans; Security awareness training; Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities; Remedial activities, processes and reporting for deficiencies; Incident detection, reporting and response; and, Continuity of operations for IT systems.

III. SAS 70 Audits

Statement on Auditing Standards (SAS) No. 70, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS

70 audit or service auditor's examination is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 Audit.

IV. Penetration/EVA

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the General Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM), dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal Government domain.

For purposes of this engagement, a network vulnerability assessment is the systematic examination of an information system, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques which may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

Table of Contents

TYPES OF AUDITS

I. CFO/EDP Audit Acts

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

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

One overall report is created for each site audited with the final report being issued by the OIG.

Site Selection Criteria

Selection of sites to be included in the CFO Act audits is primarily based on the volume of claims processed, prior findings and significance of processing done. Smaller sites are rotated into the testing to ensure their controls are also understood, but such sites are not likely to be audited every year. Because of the new requirements of the security evaluations set forth in Section 912 of the Medical Modernization Act (MMA) (see section two of this guide for more detail), the need to rotate smaller sites into testing samples may diminish in the future.

Audit Steps and Objectives

The Office of the Inspector General (OIG) of the Department of Health and Human Services performs audit work on the following areas of FISCAM during their audits:

Physical Access Controls

AC-1 Classify information resources according to their criticality and sensitivity.
- AC-1.1 Resource classifications and related criteria have been established.
- AC-1.2 Owners have classified resources.

AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
- AC-3.1 Adequate physical security controls have been implemented.
  - AC-3.1.A Physical safeguards have been established that are commensurate with the risks of physical damage or access.
  - AC-3.1.B Visitors are controlled.
- AC-3.4 Sanitation of equipment and media prior to disposal or reuse.

Entity Wide Security Program

SP-1 Periodically assess risks.
- SP-1.1 Risks are periodically assessed.

SP-2 Document an entity wide security program plan.
- SP-2.1 A security plan is documented and approved.
- SP-2.2 The plan is kept current.

SP-3 Establish a security management structure and clearly assign security responsibilities.
- SP-3.1 A security management structure has been established.
- SP-3.2 Information security responsibilities are clearly assigned.
- SP-3.3 Owners and users are aware of security policies.
- SP-3.4 An incident response capability has been implemented.

SP-4 Implement effective security-related personnel policies.
- SP-4.1 Hiring, transfer, termination, and performance policies address security.
- SP-4.2 Employees have adequate training and expertise.

SP-5 Monitor the security program's effectiveness and make changes as needed.
- SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them.
- SP-5.2 Management ensures that corrective actions are effectively implemented.

Segregation of Duties

SD-1 Segregate incompatible duties and establish related policies.
- SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties.
- SD-1.2 Job descriptions have been documented.
- SD-1.3 Employees understand their duties and responsibilities.

SD-2 Establish access controls to enforce segregation of duties.
- SD-2.1 Physical and logical access controls have been established.
- SD-2.2 Management reviews effectiveness of control techniques.

SD-3 Control personnel activities through formal operating procedures and supervision and review.
- SD-3.1 Formal procedures guide personnel in performing their duties.
- SD-3.2 Active supervision and review are provided for all personnel.

Service Continuity

SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.
- SC-1.1 Critical data and operations are identified and prioritized.
- SC-1.2 Resources supporting critical operations are identified.

SC-1.3 Emergency processing priorities are established.

SC-2 Take steps to prevent and minimize potential damage and interruption.
SC-2.1 Data and program backup procedures have been implemented.
SC-2.2 Adequate environmental controls have been implemented.
SC-2.3 Staff have been trained to respond to emergencies.
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.

SC-3 Develop and document a comprehensive contingency plan.
SC-3.1 An up-to-date contingency plan is documented.
SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.

SC-4 Periodically test the contingency plan and adjust it as appropriate.
SC-4.1 The plan is periodically tested.
SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.

The CMS contracted auditor performs audit work on the following areas of FISCAM as part of the CFO Act audits:

Access Controls

AC-2 Maintain a current list of authorized users and their access authorized.
AC-2.1 Resource owners have identified authorized users and their access authorized.
AC-2.2 Emergency and temporary access authorization is controlled.
AC-2.3 Owners determine disposition and sharing of data.

AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
AC-3.2. Adequate logical access controls have been implemented. (see also EVA)
AC-3.2.A Passwords, tokens, or other devices are used to identify and authenticate users.
AC-3.2.B Identification of access paths.
AC-3.2.C Logical controls over data files and software programs.
AC-3.2.D Logical controls over a database.
AC-3.2.E Logical controls over telecommunications access.
AC-3.3 Cryptographic tools. (see also EVA)

AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.
AC-4.1 Audit trails are maintained.
AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.
AC-4.3 Suspicious access activity is investigated and appropriate action is taken.

Application Software Development and Change Control

CC-1 Processing features and program modifications are properly authorized.
- CC-1.1 A system development life cycle methodology (SDLC) has been implemented.
- CC-1.2 Authorizations for software modifications are documented and maintained,
- CC-1.3 Use of public domain and person software is restricted.

CC-2 Test and approve all new and revised software.
- CC-2.1 Changes are controlled as programs progress through testing to final approval.
- CC-2.2 Emergency changes are promptly tested and approved.
- CC-2.3 Distribution and implementation of new or revised software is controlled,

CC-3 Control software libraries
- CC-3.1 Programs are labeled and inventoried.
- CC-3.2 Access to program libraries is restricted.
- CC-3.3 Movement of programs and data among libraries is controlled.

System Software

SS-1 Limit access to system software.
- SS-1.1 Access authorizations are appropriately limited.
- SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths.

SS-2 Monitor access to and use of system software.
- SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.
- SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.

SS-3 Control system software changes.
- SS-3.1 System software changes are authorized, tested, and approved before implementation.
- SS-3.2 Installation of system software is documented and reviewed.

Testing Procedures

Please refer to Appendix II for detailed testing procedures.

Documentation

Documentation needed by the OIG for a CFO Act Audit usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

1. Entity wide security programs (e.g. System Security Plan).
2. Network diagrams.
3. Risk assessments and vulnerability analyses.
4. Organizational charts which include names and titles for the Medicare, information systems (IS) and IS security departments.

5. Completed Core Set of Security Requirements using the CMS contractor self assessment tool (CAST).
6. Risk Assessment policies and any internal risk analysis documentation
7. Documentation on data and resource classification
8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
9. The most recent SAS 70 and risk assessment reports
10. Policies and procedures regarding conduct in the data center
11. Policies and procedures for back-up tape rotation and off-site storage
12. Policies and procedures for sanitation of media prior to disposal
13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
15. Layout of company buildings and overview of operations in each building
16. Employee lists for Medicare, IS and IS security departments (lists should include: name or identification (ID) number, job title, department, start date, and position effective date)
17. Documentation of new hire/IS security training program
18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas
19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract
20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.
21. Policies and procedures regarding the testing of the plan
22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable
23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

Documentation needed by the CMS contracted auditor for a CFO Act Audit usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

Logical Access Controls

Information on logical access controls, including the following:
NOTE: Detailed reports will vary based on security software in use, i.e. RACF, Top Secret, ACF2, UNIX, NT, etc.

1. Security policies, standards, and procedures for:

    a. Creation, modification, and deletion of user-IDs, functional groups, etc.
    b. Periodic review of access
    c. Dial-up access
    d. Use and monitoring of emergency or temporary access (Fire-call IDs)
    e. Password composition/mask

   f. Violation and security monitoring
   g. Archiving, deleting, or sharing data files
   h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)
2. List of all terminations during the current fiscal year
3. List of all transfers during the current fiscal year
4. List of all new hires during the current fiscal year
5. List of all Medicare application users
6. List of all users with dial up access
7. List of all users with the ability to change security settings (administrators)
8. Access to access requests and authorizations (for a sample of users)
9. List of access request approvers
10. Documentation supporting recertification of users
11. List of emergency or temporary (fire-call) IDs
12. Activity log of emergency or temporary IDs
13. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties
14. System default password requirements
15. Use of generic, group or system IDs
16. Database security requirements and settings
17. Security violation logging and monitoring
18. Evidence of review of user templates and/or profiles
19. Evidence of automatic timeout on terminals
20. Database access lists
21. Evidence supporting resolution of prior year audit findings

Systems Software

Systems Software information including:

1. Results of CA_EXAMINE runs
2. Policies and procedures for restricting access to systems software
3. A list of all system programmers
4. A list of all application programmers
5. A list of all computer operators
6. Results of the last review of system programmer access capabilities
7. A list of all vendor supplied software that indicates how current the software is
8. If available, integrity statements from vendors for all third party software
9. Policies and procedures for using and monitoring use of system utilities
10. Policies and procedures for identifying, selecting, installing and modifying system software
11. Policies and procedures for disabling vender supplied defaults
12. Roles and responsibilities for system programmers
13. Policies and procedures for emergency software changes
14. A list of all systems software changes made during the fiscal year
15. A list of all emergency changes made during the fiscal year
16. A list of all current access to system software
17. A list of all users with access to migrate programs to production
18. A sample of audit logs for system utilities and system programmer activity

19. Evidence of review of logs and follow up action taken
20. Initial Program Load (IPL) procedures
21. Log from last IPL

Application Development and Change Management

Information on change management, including the following:

1. System Development Life Cycle (SDLC) methodology document
2. A list of all changes made during the current fiscal year
3. Dates of and training materials from the most
4. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
5. A list of all authorized change request approvers
6. Policies and procedures over the use of personal and public domain software:
7. Test plan standards
8. A log of ABENDS
9. Procedures for new software distribution
10. Policies and procedures for emergency changes
11. A list of all emergency changes during the current fiscal year
12. Identification of virus software in use
13. A list of all users with access to library management software
14. A list of all users with access to the production libraries (production code, source code, extra program copies)
15. Tape library logs for the most recent 3 months

Interviews required

The CMS contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the Corrective Action Plan (CAP)
3. Person responsible for IT Risk Assessment
4. Person responsible for the Systems Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. Human resources (HR) contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. Local Area Network (LAN) administrator
11. Network (LAN) security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security

17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:

    a. Fiscal Intermediary Standard System (FISS)
    b. MultiCarrier System/Mandatory Claim Submission System (MCS)
    c. VIPS Medicare System (VMS)

Space and equipment requirements

1. Sufficient office space for eight people.
    a. The CMS contracted auditor will have five people on site for the CFO Act audit – one site leader, three staff, and one security specialist.
    b. OIG will have three individuals onsite for the CFO Act audit.
2. At least five high speed lines to connect to e-mail and share information.
3. Access to copier, fax machine, and printer.

II. Section 912 Evaluation

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

The CMS contracted auditor has agreed to perform procedures established by the Centers for Medicare & Medicaid Services, Office of Information Services (CMS) and the U.S. Department of Health and Human Services, Office of Inspector General (OIG) associated with the eight FISMA statutory areas which include: Periodic risk assessments; Policies and procedures based on risk assessments that cost-effectively reduce risk to an acceptable level and ensure security is addressed within the Systems Development Life Cycle and complies with the National Institute of Standards and Technology standards; Systems security plans; Security awareness training; Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities; Remedial activities, processes and reporting for deficiencies; Incident detection, reporting and response; and, Continuity of operations for IT systems.

Site Selection Criteria

All Fiscal Intermediaries and Carriers are required to have a section 912 evaluation annually.

Audit Steps and Objectives

Risk Assessments

1. Determine if the current system configuration is documented, including links to other systems.
2. Determine if risk assessments are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.
3. Determine if data sensitivity and integrity of the data have been documented and if data have been classified.
4. Determine if threat sources, both natural and manmade, have been formally identified
5. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.
6. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.
7. Determine if final risk determinations and related management approvals have been documented and maintained on file.
8. Determine if a mission/business impact analysis have been conducted and documented.
9. Obtain management's list of additional controls that have been identified to mitigate identified risks.

Policies and procedures to reduce risk

1. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in the Risk Assessments section above.
2. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.
3. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.
4. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.
5. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.
6. Determine if security policies and procedures include controls to address platform security configurations, and patch management.

Review of systems security plans

1. Determine if a security plan is documented and approved.
2. Determine if the plan is kept current.
3. Determine if a security management structure has been established.
4. Determine if information security responsibilities are clearly assigned.
5. Determine if owners and users are aware of security policies.
6. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications
7. Determine if hiring, transfer, termination and performance policies address security.
8. Determine if employee background checks are performed.
9. Determine if security employees have adequate security training and expertise.
10. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.
11. Determine if management ensures that corrective actions are effectively implemented.

Review of security awareness training

1. Determine if employees have received a copy of the Rules of Behavior.
2. Determine if employee training and professional development has been documented and formally monitored.
3. Determine if there is mandatory annual refresher training for security.
4. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.
5. Determine if employees have received a copy of or have easy access to agency security procedures and policies.
6. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.

Review of periodic testing and evaluation of the effectiveness of IT security policies

1. Determine if management reports for the review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.
2. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.
3. Determine if remedial action is being taken for issues noted on audits.

Review of remedial activities, processes and reporting for deficiencies

1. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses
2. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.
3. Determine the number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.

Review of incident detection, reporting and response

1. Determine that management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.
2. Determine if management has procedures to take and has taken action in response to unusual activity, intrusion attempts and actual intrusions.
3. Determine that management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.

Policies and procedures for continuity of operations and related physical security safeguards for IT systems.

1. Determine if critical data and operations are formally identified and prioritized.
2. Determine if resources supporting critical operations are identified in contingency plans.
3. Determine if emergency processing priorities are established.
4. Determine if data and program backup procedures have been implemented.
5. Determine if adequate environmental controls have been implemented.
6. Determine if staff has been trained to respond to emergencies.
7. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.
8. Determine if policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.
9. Determine if an up-to-date contingency plan is documented.
10. Determine if arrangements have been made for alternate data processing and telecommunications facilities.
11. Determine if the plan is periodically tested.
12. Determine if the results are analyzed and contingency plans adjusted accordingly.
13. Determine if physical security controls exist to protect IT resources.

Testing Procedures

Please refer to Appendix III for detailed testing procedures.

Documentation

Documentation needed for Section 912 includes, but is not limited to the following areas:

Risk Assessment Review

1. Current system configurations documentation including links to other systems
2. Risk assessments
3. Data classification policies/procedures
4. Threat source documentation (manmade/natural)
5. Documented system vulnerabilities, system flaws or weaknesses
6. Risk determinations (assessments) w/related management approvals
7. Mission/business impact analysis

Policies & Procedures

1. IT Security
2. Job descriptions for management

Systems Security Plan

1. Security plan
2. Security management structure
3. IS job responsibilities
4. Hiring, termination, transfer policies/procedures
5. Background check policies/procedures
6. Security policy/procedure updates
7. Management review of corrective actions

Review of Security Awareness Training

1. Training/professional development policies/procedures
2. Training schedule (if applicable)
3. Awareness posters, booklets, newsletters, etc
4. List of security professionals (pick sample)

Review of periodic testing and evaluation of the effectiveness of IT security policies and procedures including network assessments and penetration activities

1. Management reports for review & testing of IT security policies & procedures
2. Independent audit reports and evaluations

Review of remedial activities, processed and reporting for deficiencies

1. Tracking of weaknesses (Database (DB), paper, etc)
2. Planned corrective actions
3. Corrective Action Plan (CAP)
4. List of IT security weaknesses including dates of corrective actions

Review of incident detection, reporting and response

1. Policies/procedures for monitoring systems & the network
2. Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions

Review of policies and procedures for continuity of operations and related physical security safeguards for IT systems.

1. Current Recovery Plan (COOP and DR)
2. Policies/procedures for continuity of operations and related physical security safeguards for IT systems.
3. Testing results for contingency plans.

Interviews required

The CMS contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the Corrective Action Plan (CAP)
3. Person responsible for IT Risk Assessment
4. Person responsible for the Systems Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. Human resources (HR) contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. Local Area Network (LAN) administrator
11. Network (LAN) security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:

    a. Fiscal Intermediary Standard System (FISS)
    b. MultiCarrier System/Mandatory Claim Submission System (MCS)

c. VIPS Medicare System (VMS)

Space and equipment requirements

1. Sufficient office space for five people. The CMS contracted auditor will have five people on site for the 912 review – One site leader and four staff
2. At least five high speed lines to connect to e-mail and share information.
3. Access to copier, fax machine, and printer.

The first week will be for initial fieldwork and the second week will be to address any open items and complete follow-up work.

III. SAS 70 Audits

Statement on Auditing Standards (SAS) No. 70, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 Audit.

Site Selection Criteria

SAS 70 covers scope and processing; therefore, the sites with the main processing centers will be rotated into the audit program.

Audit Steps and Objectives

The planned focus of the audit team is collecting information through inquiry, inspection and observation

The CMS contracted auditor will assess the effectiveness of the controls in place as represented by management's description of controls. Management's control objectives should be aligned with key FISCAM areas. These key areas include:

- Entity-wide Security Program
- Access Controls
- Control of Application Development and Implementation
- Systems Software
- Service Continuity
- Segregation of Duties

Typically the CMS contracted auditor will assess the following (and other) control activities; contingent upon them being listed in management's description of controls:

A.1 An entity-wide security program has been documented, approved and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure and clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness and ensure security officer training and employee security awareness.

A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual and temporary) and include termination and transfer procedures that require exit interviews, return of property, such as keys and ID cards, notification to security management of terminations, removal of access to systems and escorting of terminated employees out of the facility.

A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.

A.4 Access to computerized applications, systems software and Medicare data are appropriately authorized, documented and monitored and includes approval by resource owners, procedures to control emergency and temporary access and procedures to share and properly dispose of data.

A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.

A.6 Physical access by all employees, including visitors, to Medicare facilities, data centers and systems is appropriately authorized, documented, and access violations are monitored and investigated.

A.7 Medicare application and related systems software development and maintenance activities are authorized, documented, tested, and approved.

A.8 A System Development Life Cycle methodology is documented and in use and includes planning for and costs for security requirements in systems.

A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.

A.10 Access to program libraries is properly restricted and movement of programs among libraries is controlled.

A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.

A.12 Activities of employees should be controlled via formal operating procedures that include monitoring of employee activities by management with documentation maintained to provide evidence of management's monitoring and review process.

A.13 A regular risk assessment of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.

A.14 A centralized risk management focal point for IT risk assessment has been established that includes promotion awareness programs, processes and procedures to mitigate risks and monitoring processes to assess the effectiveness of risk mitigation programs.

A.15 A risk assessment and systems security plan has been documented, approved, and monitored by management in accordance with the CMS Risk Assessment and Systems Security Plan Methodologies.

A.16 Regularly scheduled processes required to support the Medicare Contractor's continuity of operations (data, facilities or equipment) are performed.

A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components and operations.
A.18 Management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.
A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts and actual intrusions.
A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the Federal Information Security Management Act (FISMA)

Testing Procedures

Please refer to Appendix IV for detailed testing procedures.

Documentation

Documentation needed for SAS 70 is specific to the control activities defined by management at each contractor site but may include the following:

1. Entity wide security programs (e.g. System Security Plan)
2. Network diagrams
3. Risk assessments and vulnerability analyses
4. Organizational charts which include names and titles for the Medicare, information systems (IS) and IS security departments
5. Completed Core Set of Security Requirements using the CMS contractor self assessment tool (CAST)
6. Risk Assessment policies and any internal risk analysis documentation
7. Documentation on data and resource classification
8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
9. The most recent SAS 70 and risk assessment reports
10. Policies and procedures regarding conduct in the data center
11. Policies and procedures for back-up tape rotation and off-site storage
12. Policies and procedures for sanitation of media prior to disposal
13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
15. Layout of company buildings and overview of operations in each building
16. Employee lists for Medicare, IS and IS security departments (lists should include: name or identification (ID) #, job title, department, start date, and position effective date)
17. Documentation of new hire/IS security training program
18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas
19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract

20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.
21. Policies and procedures regarding the testing of the plan
22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable
23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan
24. Security policies, standards, and procedures for:

    a. Creation, modification, and deletion of user-IDs, functional groups, etc.
    b. Periodic review of access
    c. Dial-up access
    d. Use and monitoring of emergency or temporary access (Fire-call IDs)
    e. Password composition/mask
    f. Violation and security monitoring
    g. Archiving, deleting, or sharing data files
    h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)

25. List of all terminations during the current fiscal year
26. List of all transfers during the current fiscal year
27. List of all new hires during the current fiscal year
28. List of all Medicare application users
29. List of all users with dial up access
30. List of all users with the ability to change security settings (administrators)
31. Access to access requests and authorizations (for a sample of users)
32. List of access request approvers
33. Documentation supporting recertification of users
34. List of emergency or temporary (fire-call) IDs
35. Activity log of emergency or temporary IDs
36. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties
37. System default password requirements
38. Use of generic, group or system IDs
39. Database security requirements and settings
40. Security violation logging and monitoring
41. Evidence of review of user templates and/or profiles
42. Evidence of automatic timeout on terminals
43. Database access lists
44. Evidence supporting resolution of prior year audit findings
45. Results of CA_EXAMINE runs
46. Policies and procedures for restricting access to systems software
47. A list of all system programmers
48. A list of all application programmers
49. A list of all computer operators
50. Results of the last review of system programmer access capabilities
51. A list of all vendor supplied software indicating the current version of the software

52. If available, integrity statements from vendors for all third party software
53. Policies and procedures for using and monitoring use of system utilities
54. Policies and procedures for identifying, selecting, installing and modifying system software
55. Policies and procedures for disabling vender supplied defaults
56. Roles and responsibilities for system programmers
57. Policies and procedures for emergency software changes
58. A list of all systems software changes made during the fiscal year
59. A list of all emergency changes made during the fiscal year
60. A list of all current access to system software
61. A list of all users with access to migrate programs to production
62. A sample of audit logs for system utilities and system programmer activity
63. Evidence of review of logs and follow up action taken
64. Initial Program Load (IPL) procedures
65. Log from last IPL
66. System Development Life Cycle (SDLC) methodology document
67. Change control policies and procedures (if not included in the SDLC document)
68. A list of all changes made during the current fiscal year
69. Dates of and training materials from the most recent SDLC training class
70. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
71. A list of all authorized change request approvers
72. Policies and procedures over the use of personal and public domain software:
73. Test plan standards
74. A log of abends
75. Procedures for new software distribution
76. Policies and procedures for emergency changes
77. A list of all emergency changes during the current fiscal year
78. Identification of virus software in use
79. A list of all users with access to library management software
80. A list of all users with access to the production libraries (production code, source code, extra program copies)
81. Tape library logs for the most recent 3 months
82. Current system configurations documentation including links to other systems
83. Threat source documentation (manmade/natural)
84. Documented system vulnerabilities, system flaws or weaknesses
85. Mission/business impact analysis
86. Job descriptions for management
87. IS job responsibilities
88. Background check policies/procedures
89. Security policy/procedure updates
90. Management review of corrective actions
91. Training/professional development policies/procedures
92. Training schedule (if applicable)
93. Awareness posters, booklets, newsletters, etc
94. Management reports for review & testing of IT security policies & procedures
95. Independent audit reports and evaluations

96. Tracking of weaknesses (DB, paper, etc)
97. Planned corrective actions
98. CAP
99. List of IT security weaknesses including dates of corrective actions
100. Policies/procedures for monitoring systems & the network
101. Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions

Interviews required

The CMS contracted auditor shall interview the following Medicare contractor employees:

1. Medicare compliance officer
2. Person responsible for the Corrective Action Plan (CAP)
3. Person responsible for IT Risk Assessment
4. Person responsible for the Systems Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. Human resources (HR) contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. Local Area Network (LAN) administrator
11. Network (LAN) security officer
12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:

    a. Fiscal Intermediary Standard System (FISS)
    b. MultiCarrier System/Mandatory Claim Submission System (MCS)
    c. VIPS Medicare System (VMS)

Space and equipment requirements

1. Sufficient office space for six people. The CMS contracted auditor will have six people on site for the SAS 70 audit – Four staff (senior associate/associate), one expert, and one manager
2. At least six high speed lines to connect to e-mail and share information.
3. Access to copier, fax machine, and printer.

The CMS contracted auditor auditors shall stay six weeks over a 3-4 month period to complete the audit

IV. Penetration/EVA

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO Federal Information System Controls Audit Manual (FISCAM), dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal Government domain.

For purposes of this engagement, a network vulnerability assessment is the systematic examination of an information system, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques which may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

Execution of the Audit

Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results. The testing includes procedures to demonstrate both external and internal threats. To ensure that the integrity of the testing is not impaired, parties with knowledge of the testing are requested to restrict communicating any aspects, including test schedules to individuals at the operational level prior to or during test performance.

The CMS contracted auditor is the Independent Public Accountant (IPA) engaged by the Office of the Inspector General (OIG) Department of Health and Human Services (HHS) to perform testing at third party CMS contractors as part of the FY 2004 Financial Statement Audit of the Centers for Medicare and Medicaid Services ("CMS").
There will be a site summary that includes a high level description of the testing performed and findings describing technical issues identified during testing. The findings will be written in terms of Condition, Cause, Criteria, Effect, and Recommendation (following GAO Yellow Book guidelines). The Site Summary will be supported by summary work papers for each type of testing performed.

Site Selection Criteria

Sites are included in the CFO Act audits primarily based on the volume of claims processed, prior findings and significance of processing done. Smaller sites are rotated into the testing to ensure their controls are also understood, but such sites are not likely to be audited every year.

Audit Steps and Objectives

Steps to perform penetration testing

Phase 1 – Assess & Model Threats

The Assess & Model Threats phase is used to establish and acquire the information required to successfully define the scope of the security penetration testing. This involves gathering information and completing an initial threat analysis to ensure that testing emulates the threats that are of real concern to the organization. This includes project start-up, information gathering and threat analysis.

1. Threat analysis is usually conducted according to prescribed scenarios that are clearly documented in the Statement of Work. Some common threat scenarios for an external penetration test include:
    a. Untrusted Outsider – This is the most common scenario for an External (Internet) penetration test. This scenario is designed to simulate individuals with no significant knowledge of the client's computing operations that are attempting to gain access from remote locations;
    b. Trusted Outsider – This scenario is designed to simulate third parties (e.g. customers, suppliers, partners) that have limited legitimate access to the client's network. In the event of the trusted outsider scenario, establish with the client what resources the team will attack and arrange for the client to set up valid credentials to access those resources (e.g. usernames/passwords, SecurID tokens).
2. During the project start-up, agree on primary contacts for both the CMS contracted auditor and the client to contact in case of an emergency. These contact numbers should be accessible at all times during testing. All members of the team should be aware of the escalation path and procedures during testing.
3. Determine with the client when testing should stop. Some clients request that as soon as access is obtained, the CMS contracted auditor stop and notify the client before attempting to obtain further access to resources.
4. Determine if there are specific targets of interest that the CMS contracted auditor should direct attacks to (e.g. a focus on the client's web server).
5. All penetration activities must be conducted from either a CMS contracted auditor lab or the client site. Identify the source IP range you will be using with the client to allow them to differentiate the CMS contracted auditor activities from legitimate hacking attempts. Contact your lab manager for information on your external IP address range.
6. Establish acceptable timeframes for penetration testing with the client to avoid disrupting day-to-day client business (and to avoid being caught if the engagement requires stealth testing).
7. Inquire about any IP addresses that should be excluded from testing.

Phase 2 – Survey Testing

The Survey Testing phase is used to identify and document client devices that may be accessed from the Internet and to determine if any of these devices might be vulnerable to well-known exploits. This includes gathering IP address, MAC address, operating system, web server, application, and enticement information, in addition to any other salient information about the target environment.

1. Identify Internet connections and IP ranges by querying public databases.
2. Identify salient target information available in newsgroups and web pages.
3. Use DNS queries to identify client networks and systems. These queries are best performed from a UNIX system that has the dig utility installed (NOTE: dig is also available for Windows systems). IP addresses that are found through DNS queries should be looked up in the Internet repositories listed above to determine the range and owner of the IP address. The following queries can be used to identify client systems and networks:
4. Once you have identified client IP ranges and accessible websites, confirm IP addresses with the client contact before attempting to attack any systems.
    a. Once the client has approved the IP ranges identified during the first part of this phase, scans can be conducted using a map to identify open ports and potential attack points on each of the servers in the range. Depending on the requirements of the organization, different types of scans may be used to try and avoid detection.
5. Once the initial scan is complete, a table should be created for the information gathered from each port.
6. After you have identified the services running on each port and obtained all information possible, the Intrusion Testing Phase of the engagement can begin. Note: confirm with the engagement manager before beginning Intrusion testing to determine if the client needs to be notified before beginning.

Phase 3 – Intrusion Testing

The Intrusion Testing phase is used to examine the weaknesses found and, where appropriate, attempt to exploit these weaknesses to demonstrate the risks and exposures. This stage is the core of the security penetration test and may be an iterative process as one exploited weakness may give rise to further exploitation opportunities.

The overall goal of the Intrusion Testing phase is to demonstrate access to systems and the capability to exploit this access further, not necessarily to gain full uncontrolled access to systems, although there may be instances where such access may be permissible.

1. Each attempt you make to gain access to systems (including every username and password combination) **must be documented**. There are an infinite number of avenues to attempt to gain access to a system, but the intrusion attempts should be performed in the following order.
2. If you gain access to a system, **take a screen shot** and **SLOW DOWN**.
3. Navigate the filesystem and attempt to identify any sensitive data files. These may include usernames, passwords or SMTP strings.
4. Use the machine as a “stepping stone” and exploit any trust relationships to compromise additional machines. Determine any network interfaces this system has (e.g. network interface cards) and determine what capabilities the system gives you (e.g. ping internally, telnet). Further system testing, such as this, should be conducted according to the same procedures prescribed so far: (1) Assess and Model Threats; (2) Survey Testing; and (3) Intrusion Testing.

Phase 4 – Assess Exposures

Throughout the assessment, the practitioner should consistently document any actions and findings. The assess exposures phase (reporting phase) brings together this information in a presentable format and draws conclusions about the impact of each finding to the business. This stage requires an analysis of the data to provide actionable, reasonable information to the client.

Documentation

Documentation and other items needed for Penetration/External Vulnerability Assessment (EVA) includes, but is not limited to:

1. Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.
2. Site / system password policies
3. Applicable phone number range for dial-up "war-dialing" testing.
4. Applicable Internet Protocol (IP) address spaces for penetration testing.
5. Listing of IP addresses assigned to, or under the purview of the site.
6. Listing of prohibited telephones/systems/networks
7. Standards and Guidelines (Risk Model) for system configuration.

Additional Penetration/EVA items include:

1. Personnel to observe the penetration and diagnostic testing activities (if desired by the auditee).
2. Permission to connect the CMS contracted auditor laptop to site's network (while monitored).
3. Network access for internal testing.
   System administrator/programmer access for systems to perform diagnostic review.
4. Specific documents required by The CMS contracted auditor will be requested in the Provided by Client (PBC) list. This list will be provided prior to the start of testing.

Interviews required

1. An individual from the Security Department
2. CMS Contact
3. Someone knowledgeable of the CMS environment
4. Systems Administrator
5. Network Administrator
6. Database Administrator
7. Firewall Administrator

Space and equipment requirements

1. Workspace for each member of the audit team – usually one Senior Associate and one Associate

2. At least 1 telephone line, and network connectivity.

The CMS contracted auditor auditors will typically stay 3-5 days, depending upon the readiness of the contractor.

APPENDIX I: SYNOPSIS OF DOCUMENTATION REQUIRED

This Chart Provides a Synopsis of Documentation Required

Documentation	CFO Audit	Section 912	SAS 70	EVA
Entity wide security programs (e.g. System Security Plan)	✔	✔	✔	
Network diagrams	✔	✔	✔	✔
Risk assessments and vulnerability analyses	✔	✔	✔	
Organizational charts which include names and titles for the Medicare, information systems (IS) and IS security departments	✔	✔	✔	
Completed Core Set of Security Requirements using the CMS contractor self assessment tool (CAST)	✔	✔	✔	
Risk Assessment policies and any internal risk analysis documentation	✔	✔	✔	
Documentation on data and resource classification	✔	✔	✔	
HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations	✔	✔	✔	
The most recent SAS 70 and risk assessment reports	✔		✔	
Policies and procedures regarding conduct in the data center	✔		✔	
Policies and procedures for back-up tape rotation and off-site storage	✔	✔	✔	
Policies and procedures for sanitation of media prior to disposal	✔	✔	✔	
Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms	✔		✔	
Policies and procedures regarding visitors to both the general campus and to the sensitive areas	✔		✔	
Layout of company buildings and overview of operations in each building	✔		✔	
Employee lists for Medicare, IS and IS security departments (lists should include: name or identification (ID) #, job title, department, start date, and position effective date)	✔	✔	✔	
Documentation of new hire/IS security training program	✔	✔	✔	
Vendor sign in and sign out logs for maintenance or repairs in sensitive areas	✔		✔	
Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.	✔	✔	✔	
Policies and procedures regarding the testing of the plan	✔	✔	✔	
Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable	✔	✔	✔	
Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan	✔	✔	✔	
Security policies, standards, and procedures for:				
• Creation, modification, and deletion of user-IDs, functional groups, etc.	✔		✔	
• Periodic review of access	✔		✔	
• Dial-up access	✔		✔	
• Use and monitoring of emergency or temporary access (Fire-call IDs)	✔		✔	
• Password composition/mask	✔		✔	✔
• Violation and security monitoring	✔		✔	
• Archiving, deleting, or sharing data files	✔		✔	
• Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)	✔		✔	
List of all terminations during the current fiscal year	✔		✔	
List of all transfers during the current fiscal year	✔		✔	
List of all new hires during the current fiscal year	✔		✔	
List of all Medicare application users/	✔	✔	✔	
List of all users with dial up access	✔		✔	
List of all users with the ability to change security settings (administrators)	✔		✔	
Access to access requests and authorizations (for a sample of users)	✔		✔	
List of access request approvers	✔		✔	
Documentation supporting recertification of users	✔		✔	
List of emergency or temporary (fire-call) IDs	✔		✔	
Activity log of emergency or temporary IDs	✔		✔	
Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties	✔		✔	
System default password requirements	✔		✔	
Use of generic, group or system IDs	✔		✔	
Database security requirements and settings	✔		✔	
Security violation logging and monitoring	✔		✔	
Evidence of review of user templates and/or profiles	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Evidence of automatic timeout on terminals	✔		✔	
Database access lists	✔		✔	
Evidence supporting resolution of prior year audit findings	✔		✔	
Results of CA_EXAMINE runs	✔		✔	
Policies and procedures for restricting access to systems software	✔		✔	
A list of all system programmers	✔		✔	
A list of all application programmers	✔		✔	
A list of all computer operators	✔		✔	
Results of the last review of system programmer access capabilities	✔		✔	
A list of all vendor supplied software that indicates how current the software is	✔		✔	
If available, integrity statements from vendors for all third party software	✔		✔	
Policies and procedures for using and monitoring use of system utilities	✔		✔	
Policies and procedures for identifying, selecting, installing and modifying system software	✔		✔	
Policies and procedures for disabling vender supplied defaults	✔		✔	
Roles and responsibilities for system programmers	✔		✔	✔
Policies and procedures for emergency software changes	✔		✔	
A list of all systems software changes made during the fiscal year	✔		✔	
A list of all emergency changes made during the fiscal year	✔		✔	
A list of all current access to system software	✔		✔	
A list of all users with access to migrate programs to production	✔		✔	
A sample of audit logs for system utilities and system programmer activity	✔		✔	
Evidence of review of logs and follow up action taken	✔		✔	
Initial Program Load (IPL) procedures	✔		✔	
Log from last IPL	✔		✔	
System Development Life Cycle (SDLC) methodology document	✔	✔	✔	
Change control policies and procedures (if not included in the SDLC document)	✔		✔	
A list of all changes made during the current fiscal year	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Dates of and training materials from the most recent SDLC training class	✔		✔	
Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)	✔		✔	
A list of all authorized change request approvers	✔		✔	
Policies and procedures over the use of personal and public domain software:	✔		✔	
Test plan standards	✔		✔	
A log of ABENDS	✔		✔	
Procedures for new software distribution	✔		✔	
Policies and procedures for emergency changes	✔		✔	
A list of all emergency changes during the current fiscal year	✔		✔	
Identification of virus software in use	✔		✔	
A list of all users with access to library management software	✔		✔	
A list of all users with access to the production libraries (production code, source code, extra program copies)	✔		✔	
Tape library logs for the most recent 3 months	✔		✔	
Current system configurations documentation including links to other systems		✔	✔	
Threat source documentation (manmade/natural)		✔	✔	
Documented system vulnerabilities, system flaws or weaknesses		✔	✔	
Mission/business impact analysis		✔	✔	
Job descriptions for management		✔	✔	
IS job responsibilities		✔	✔	
Background check policies/procedures		✔	✔	
Security policy/procedure updates		✔	✔	
Management review of corrective actions		✔	✔	
Training/professional development policies/procedures		✔	✔	
Training schedule (if applicable)		✔	✔	
Awareness posters, booklets, newsletters, etc		✔	✔	
Management reports for review & testing of IT security policies & procedures		✔	✔	
Independent audit reports and evaluations		✔	✔	
Tracking of weaknesses (DB, paper, etc)		✔	✔	
Planned corrective actions		✔	✔	
All four quarter CAPs		✔	✔	
List of IT security weaknesses including dates of		✔	✔	

Documentation	CFO Audit	Section 912	SAS 70	EVA
corrective actions				
Policies/procedures for monitoring systems & the network		✔	✔	
Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions		✔	✔	
Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.				✔
Standards and Guidelines (Risk Model) for system configuration.				✔
Applicable phone number range for dial-up “war-dialing” testing.				✔
Applicable Internet Protocol (IP) address spaces for penetration testing.				✔
Listing of IP addresses assigned to, or under the purview of the site.				✔
Listing of prohibited telephones/systems/networks				✔

APPENDIX II: DETAILED CFO TESTING PROCEDURES

Control Activity	Detailed Testing
Access Control	
AC-1 Classify information resources according to their criticality and sensitivity.	
1. Resource classifications and related criteria have been established.	1. Review policies and procedures.
	2. Interview resource owners.
2. Owners have classified resources.	1. Review resource classification documentation and compare to risk assessments. Discuss any discrepancies with appropriate officials.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.	
1. Adequate physical security controls have been implemented.	
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Review a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.
	2. Walk through facilities
	3. Review risk analysis.
	4. Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access.
	5. Before becoming recognized as the auditor, attempt to access sensitive areas without escort or identification badges.
	6. Observe entries to and exits from facilities during and after normal business hours.
	7. Observe utilities access paths.
	8. Interview management.
	9. Observe entries to and exits from sensitive areas during and after normal business hours.
	10. Interview employees.
	11. Review procedures for the removal and return of storage media from and to the library.
	12. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.
	13. Observe practices for safeguarding keys and other devices.
	14. Review written emergency procedures.
	15. Examine documentation supporting prior fire drills.

	16. Observe a fire drill.
B. Visitors are controlled.	1. Review visitor entry logs.
	2. Observe entries to and exits from sensitive areas during and after normal business hours.
	3. Interview guards at facility entry.
	4. Review documentation on and logs of entry code changes.
	5. Observe appointment and verification procedures for visitors.
4. Sanitation of equipment and media prior to disposal or reuse.	1. Review written procedures.
	2. Interview personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, test that they have been appropriately sanitized.
Entity Wide Security Program	
SP-1 Risks are periodically assessed.	
1. Risks are periodically assessed.	1. Review risk assessment policies.
	2. Review the most recent high-level risk assessment.
	3. Review the objectivity of personnel who performed and reviewed the assessment.
SP-2 Document an entitywide security program plan.	
1. A security plan is documented and approved.	1. Review the security plan.
	2. Determine whether the plan covers the topics prescribed by OMB Circular A-130.
2. The plan is kept current.	1. Review the security plan and any related documentation indicating that it has been reviewed and updated and is current.
SP-3 Establish a security management structure and clearly assign security responsibilities.	
1. A security management structure has been established.	1. Review the security plan and the entity's organization chart.
	2. Interview security management staff.
	3. Review pertinent organization charts and job descriptions.
	4. Interview the security manager.
2. Information security responsibilities are clearly assigned.	1. Review the security plan.
3. Owners and users are aware of security policies.	1. Review documentation supporting or evaluating the awareness program. Observe a security briefing.

	2. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
	3. Review memos, electronic mail files, or other policy distribution mechanisms.
	4. Review personnel files to test whether security awareness statements are current.
	5. Call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.
4. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.
	2. Review documentation supporting incident handling activities.
	3. Determine qualifications of response team members.
SP-4 Implement effective security-related personnel policies.	
1. Hiring, transfer, termination, and performance policies address security.	1. Review hiring policies.
	2. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
	3. Review reinvestigation policies.
	4. For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed.
	5. Review policies on confidentiality or security agreements.
	6. For a selection of such users, determine whether confidentiality or security agreements are on file.
	7. Review vacation policies.
	8. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	9. Determine who performed vacationing employee's work during vacation.
	10. Review job rotation policies.
	11. Review staff assignment records and determine whether job and shift rotations occur.
	12. Review pertinent policies and procedures.
	13. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.
	14. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Employees have adequate training and expertise.	1. Review job descriptions for security management personnel, and for a selection of other personnel.

	2. For a selection of employees, compare personnel records on education and experience with job descriptions.
	3. Review training program documentation.
	4. Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
SP-5 Monitor the security program's effectiveness and make changes as needed.	
1. Management periodically assesses the appropriateness of security policies and compliance with them.	1. Review the reports resulting from recent assessments, including the most recent FMFIA report.
	2. Determine when last independent review or audit occurred and review results.
	3. Review written authorizations or accreditation statements.
	4. Review documentation related to corrective actions.
2. Management ensures that corrective actions are effectively implemented.	1. Review the status of prior-year audit recommendations and determine if implemented corrective actions have been tested.
	2. Review recent FMFIA reports.
Segregation of Duties	
SD-1 Segregate incompatible duties and establish related policies.	
1. Incompatible duties have been identified and policies implemented to segregate these duties.	1. Review pertinent policies and procedures.
	2. Interview selected management and IS personnel regarding segregation of duties.
	3. Review an agency organization chart showing IS functions and assigned personnel.
	4. Interview selected personnel and determine whether functions are appropriately segregated.
	5. Determine whether the chart is current and each function is staffed by different individuals.
	6. Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained.
	7. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	8. Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combination of functions.
	9. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	10. Interview management, observe activities, and test transactions.
	11. Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.

	12. Review the adequacy of documented operating procedures for the data center.
2. Job descriptions have been documented.	1. Review job descriptions for several positions in organizational units and for user security administrators.
	2. Determine whether duties are clearly described and prohibited activities are addressed.
	3. Review the effective dates of the position descriptions and determine whether they are current.
	4. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	5. Review job descriptions and interview management personnel.
3. Employees understand their duties and responsibilities.	1. Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	2. Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	3. Interview management personnel in these activities.
SD-2 Establish access controls to enforce segregation of duties.	
1. Physical and logical access controls have been established.	1. Interview management and subordinate personnel.
2. Management reviews effectiveness of control techniques.	1. Interview management and subordinate personnel.
	2. Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	3. Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews.
SD-3 Control personnel activities through formal operating procedures and supervision and review.	
1. Formal procedures guide personnel in performing their duties.	1. Review manuals.
	2. Interview supervisors and personnel.
	3. Observe processing activities.
2. Active supervision and review are provided for all personnel.	1. Interview supervisors and personnel.
	2. Observe processing activities.
	3. Review history log reports for signatures indicating supervisory review.
	4. Determine who is authorized to perform the initial program load for the system, what steps

	are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.
Service Continuity	
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.	
1. Critical data and operations are identified and prioritized.	1. Review related policies.
	2. Review list and any related documentation.
	3. Interview program, data processing, and security administration officials. Determine their input and their assessment of the reasonableness of priorities established.
2. Resources supporting critical operations are identified.	1. Review related documentation.
	2. Interview program and security administration officials.
3. Emergency processing priorities are established.	1. Review related policies.
	2. Review related documentation.
	3. Interview program and security administration officials.
SC-2 Take steps to prevent and minimize potential damage and interruption.	
1. Data and program backup procedures have been implemented.	1. Review written policies and procedures for backing up files.
	2. Compare inventory records with the files maintained off-site and determine the age of these files.
	3. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports.
	4. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	5. Locate and examine documentation.
	6. Examine the backup storage site.
2. Adequate environmental controls have been implemented.	1. Examine the entity's facilities
	2. Interview site managers.
	3. Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observe the operation, location, maintenance and access to the air cooling system.
	5. Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determine whether the activation of heat and smoke detectors will notify the fire

	department.
	7. Review test policies.
	8. Review documentation supporting recent tests of environmental controls.
	9. Review policies and procedures regarding employee behavior.
	10. Observe employee behavior.
3. Staff have been trained to respond to emergencies.	1. Interview data center staff.
	2. Review training records.
	3. Review training course documentation.
	4. Review emergency response procedures.
	5. Review test policies.
	6. Review test documentation.
	7. Interview data center staff.
4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	1. Review policies and procedures.
	2. Interview data processing and user management.
	3. Review maintenance documentation.
	4. Interview data center management.
	5. Interview senior management, data processing management, and user management.
	6. Review supporting documentation.
SC-3 Develop and document a comprehensive contingency plan.	
1 An up-to-date contingency plan is documented.	1. Review the contingency plan and compare its provisions with the most recent risk assessment and with a current description of automated operations.
	2. Interview senior management, data center management, and program managers.
	3. Review the contingency plan.
	4. Interview senior management, data center management, and program managers.
	5. Observe copies of the contingency plan held off-site.
	6. Review the plan and any documentation supporting recent plan reassessments.
2. Arrangements have been made for alternate data processing and telecommunications facilities.	1. Review contracts and agreements.
SC-4 Periodically test the contingency plan and adjust it as appropriate.	
1. The plan is periodically tested.	1. Review policies on testing.

	2. Review test results.
	3. Observe a disaster recovery test.
2. Test results are analyzed and contingency plans are adjusted accordingly.	1. Review final test report.
	2. Interview senior managers to determine if they are aware of the test results.
	3. Review any documentation supporting contingency plan adjustments.

The CMS contracted auditor will perform audit work on the following areas of FISCAM as part of the CFO Act audits

Access Controls	
AC-2 Maintain a current list of authorized users and their access authorized.	
1. Resource owners have identified authorized users and their access authorized.	1. Review pertinent written policies and procedures.
	2. For a selection of users (both application user and IS personnel) review access authorization documentation.
	3. Interview owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, review authorization and justification.
	5. Interview security managers and review documentation provided to them.
	6. Review a selection of recent profile changes and activity logs.
	7. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Review pertinent policies and procedures.
	2. Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.
	3. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examine standard approval forms.
	2. Interview data owners.
	3. Examine documents authorizing file sharing and file sharing agreements.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.	
2. Adequate logical access controls have been implemented. (see also EVA)	
A. Passwords, tokens, or other devices are used to identify and authenticate users.	1. Review pertinent policies and procedures.
	2. Interview users.
	3. Review security software password parameters.
	4. Observe users keying in passwords.
	5. Attempt to log on without a valid password; make repeated attempts to guess passwords.
	6. Assess procedures for generating and communicating passwords to users.
	7. Review a system-generated list of current passwords.

	8. Search password file using audit software.
	9. Attempt to log on using common vendor supplied passwords.
	10. Interview users and security managers.
	11. Review a list of IDs and passwords.
	12. Repeatedly attempt to log on using invalid passwords.
	13. Review security logs.
	14. Review pertinent policies and procedures.
	15. Review documentation of such comparisons.
	16. Interview security managers.
	17. Make comparison using audit software.
	18. View dump of password files (e.g., hexadecimal printout).
	19. Interview users.
	20. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.
B. Identification of access paths.	1. Review access path diagram.
C. Logical controls over data files and software programs.	1. Interview security administrators and system users.
	2. Review security software parameters.
	3. Observe terminals in use.
	4. Review a system-generated list of inactive logon IDs, and determine why access for these users has not been terminated.
	5. Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Perform penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system. These tests should be performed as (1) an "outsider" with no information about the entity's computer systems; and (2) an "outsider" with prior knowledge about the systems--e.g., an ex-insider, and (3) an "insider" with and without specific information about the entity's computer systems, and with access to the entity's facilities.
	7. When performing outsider tests, test the controls over external access to computer

	resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
	8. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determine whether naming conventions are used.
D. Logical controls over a database.	1. Review pertinent policies and procedures.
	2. Interview database administrator.
	3. Review DBMS and DD security parameters.
	4. Test controls by attempting access to restricted files.
	5. Review security system parameters.
E. Logical controls over telecommunications access.	1. Review pertinent policies and procedures.
	2. Review parameters set by communications software or teleprocessing monitors.
	3. Test telecommunications controls by attempting to access various files through communications networks.
	4. Identify all dial-up lines through automatic dialer software routines and compare with known dial-up access. Discuss discrepancies with management.
	5. Interview telecommunications management staff and users.
	6. Review pertinent policies and procedures.
	7. View the opening screen seen by telecommunication system users.
	8. Review the documentation showing changes to dial-in numbers.
	9. Review entity's telephone directory to verify that the numbers are not listed.
3 Cryptographic tools. (see also EVA)	1. To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.	
1. Audit trails are maintained.	1. Review security software settings to identify types of activity logged.
2. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Review pertinent policies and procedures.
	2. Review security violation reports.
	3. Examine documentation showing reviews of questionable activities.
3. Suspicious access activity is investigated and appropriate action is taken.	1. Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator.
	2. Interview senior management and personnel responsible for summarizing violations.
	3. Review any supporting documentation.

	4. Review policies and procedures and interview appropriate personnel.
	5. Review any supporting documentation.
Application Software Development and Change Control	
CC-1 Processing features and program modifications are properly authorized.	
1. A system development life cycle methodology (SDLC) has been implemented.	1. Review SDLC methodology.
	2. Review system documentation to verify that SDLC methodology was followed.
	3. Interview staff.
	4. Review training records.
2. Authorizations for software modifications are documented and maintained,	1. Identify recent software modifications and determine whether change request forms were used.
	2. Examine a selection of software change request forms for approvals.
	3. Interview software development staff.
3. Use of public domain and person software is restricted.	1. Review pertinent policies and procedures.
	2. Interview users and data processing staff.
CC-2 Test and approve all new and revised software.	
1. Changes are controlled as programs progress through testing to final approval.	1. Review test plan standards.
	2. For the software change requests selected for control activity CC-1.2: (1) review specifications; (2) trace changes from code to design specifications; (3) review test plans; (4) compare test documentation with related test plans; (5) analyze test failures to determine if they indicate ineffective software testing; (6) review test transactions and data.
	3. For the software change requests selected for control activity CC-1.2 (continued): (1) review test results; (2) review documentation of management or security administrator reviews; (3) verify user acceptance; and (4) review updated documentation.
	4. Determine whether operational systems experience a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
2. Emergency changes are promptly tested and approved.	1. Review procedures.
	2. For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.
3. Distribution and implementation of new or revised software is controlled,	1. Examine procedures for distributing new software.
	2. Examine implementation orders for a sample of changes.
CC-3 Control software libraries	

1. Programs are labeled and inventoried.	1. Review pertinent policies and procedures.
	2. Interview personnel responsible for library control.
	3. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures.
	4. Determine how many prior versions of software modules are maintained.
2. Access to program libraries is restricted.	1. Examine libraries in use.
	2. Interview library control personnel.
	3. Examine libraries in use.
	4. Verify that source code exists for a selection of production load modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load modules size.
	5. For critical software production programs, determine whether access control software rules are clearly defined.
	6. Test access to program libraries by examining security system parameters.
	7. Select some program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
3. Movement of programs and data among libraries is controlled.	1. Review pertinent policies and procedures.
	2. For a selection of program changes, examine related documentation to verify that: (1) procedures for authorizing movement among libraries were followed, and (2) before and after images were compared.
System Software	
SS-1 Limit access to system software.	
1. Access authorizations are appropriately limited.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel regarding access restrictions.
	3. Observe personnel accessing 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.
	5. Select some systems programmers and determine whether management-approved documentation supports their access to system software.
	6. Select some application programmers and determine whether they are not authorized access.
	7. Determine the last time the access capabilities of system programmers were reviewed.

2. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Test the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtain a list of vendor-supplied software and determine if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally review the installation of system software components and determine whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including:
	(1) Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls.
	(2) Determine whether applications interfaces have been implemented to support operating system integrity controls, including on-line transaction monitors; database software; on-line editors; on-line direct-access storage devices, on-line operating system datasets; exits related to the operating system, security, and program products; and controls over batch processing, to include security controls, scheduler controls, and access authorities.
	(3) Evaluate the controls over external access to computer resources including networks, dial-up, LAN, WAN, RJE, and the Internet.
	(4) Identify potential opportunities to adversely impact the operating system and its products through trojan horses, viruses, and other malicious actions.
	5. Obtain a list of all system software on test and production libraries used by the entity.
	6. Verify that access control software restricts access to system software.
	7. Using security software reports, determine who has access to system software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated In the presence of the auditor.
	8. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquire whether disabling has occurred.
	10. Test for default presence using vendor standard IDs and passwords.
	11. Determine what terminals are set up as master consoles and what controls exist over them.
	12. Test to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.

SS-2 Monitor access to and use of system software.	
1. Policies and techniques have been implemented for using and monitoring use of system utilities.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel regarding their responsibilities.
	3. Determine whether logging occurs and what information is logged.
	4. Review logs.
	5. Using security software reports, determine who can access the logging files.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interview technical management regarding their reviews of privileged system software and utilities usage.
	2. Review documentation supporting their reviews.
	3. Interview management and systems personnel regarding these investigations.
	4. Review documentation supporting these investigations.
	5. Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Review documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interview management and analyze their reviews concerning the use of system software.
	8. Determine what management reviews have been conducted, and their currency, over this area.
SS-3 Control system software changes.	
1. System software changes are authorized, tested, and approved before implementation.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel.
	3. Review procedures for identifying and documenting system software problems.
	4. Interview management and systems programmers.
	5. 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.
	6. Determine what authorizations and documentation are required prior to initiating system software changes.
	7. Select recent system software changes and determine whether the authorization was obtained and the change is supported by a change request document.
	8. Determine the procedures used to test and approve system software prior to its implementation.

	9. Select recent system software changes and test whether the indicated procedures were in fact used.
	10. Review procedures used to control and approve emergency changes.
	11. Select some emergency changes to system software and test whether the indicated procedures were in fact used.
2. Installation of system software is documented and reviewed.	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.
	4. Interview management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries and whether outdated versions are removed from production libraries.
	5. Review supporting documentation for some system software migrations and the removal of outdated versions from production libraries.
	6. Interview data center management about their role in reviewing system software installations.
	7. Review some recent system software installations and determine whether documentation shows that logging and management review occurred.
	8. Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.
	9. Interview management and systems programmers about the currency of system software and the currency and completeness of software documentation.
	10. Review documentation and test whether recent changes are incorporated.

APPENDIX III: DETAILED MMA 912 TESTING PROCEDURES

Control Activity	Detailed Tests
Section I: Risk Assessment Review	
A. Determine if the current system configuration is documented, including links to other systems.	1. Review the most recent system configuration
	2. Review the system configuration and/or related documentation indicating it has been reviewed and kept current
B. Determine if risk assessments are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.	1. Review the risk assessment policies
	2. Review the most recent risk assessment
	3. Review the risk assessment and/or related documentation indicating it has been reviewed and conducted annually
C. Determine if data sensitivity and integrity of the data have been documented and if data have been classified	1. Review data classification policies and procedures
	2. Review evidence based on policies and procedures that data has been classified
D. Determine if threat sources, both natural and manmade, have been formally identified	1. Review risk assessment to ensure threat sources, both natural and man-made, have been identified and documented
E. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.	1. Review the risk assessment to ensure a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed.
	2. Review the risk assessment and/or related documentation indicating it has been reviewed and kept current
F. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.	1. Review the risk assessment to ensure mitigating controls are documented.
	2. Review the risk assessment to ensure mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities
G. Determine if final risk determinations and related management approvals have been documented and maintained on file.	1. Review the risk assessment to ensure final risk determinations are documented
	2. Review risk assessment and/or related documentation indicating it has been approved (currently)

H. Determine if a mission/business impact analysis have been conducted and documented.	1. Review documented critical business processes
	2. Review mission/business impact analysis to ensure it has been documented for the critical business processes
I. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Review any additional documented lists of controls identified to mitigate identified risks.
Section II: Policies and Procedures to Reduce Risk	
A. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	1. Review the most current risk assessment
	2. Review IT Security policies and procedures to ensure they reduce the risk outlined in the risk assessment
	3. Ensure IT Security policies and procedures are current
B. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Review the most current System Development Life Cycle
	2. Review additional information (i.e., System Security Plan) which outline security controls included in the cost of developing new systems
	3. Review software change control policies and procedures to ensure changes are being controlled effectively
C. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	1. Perform inquiries of appropriate personnel regarding major systems maintained at the site.
	2. Review documentation indicating accreditations and certifications were performed for the noted systems
	3. Ensure accreditations and certifications are in compliance with FISMA policies
D. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits	1. Perform inquiries of appropriate personnel regarding systems for which controls have been tested
	2. Review evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems
	3. Review evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits
	4. Ensure all reviews have been performed within the scope of the review

E. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Review the most recent CMS CSR
	2. GAPs in compliance as documented in the CMS CSR
	3. Review management's response to the CSR to ensure proper controls are in place/are in the process of being in place
F. Determine if security policies and procedures include controls to address platform security configurations, and patch management.	1. Review platform security configuration policies and procedures
	2. Review patch management policies and procedures
Section III: Review of System Security Plans	
A. Determine if a security plan is documented and approved.	1. Review most current System Security Plan
	2. Review documentation indicating the System Security Plan was approved by appropriate individuals
B. Determine if the plan is kept current.	1. Review previous and current System Security Plan to ensure updates have been made as necessary
	2. Review the date of the most current System Security Plan to ensure it is in the scope of the review
C. Determine if a security management structure has been established.	1. Review the security management's organizational chart
D. Determine if information security responsibilities are clearly assigned.	1. Review the security management's organization chart
	2. Review the security management's formal job descriptions
E. Determine if owners and users are aware of security policies.	1. Review security training schedules
	2. Review security training materials
	3. For a selection of owners and users ensure they have attended the required trainings
F. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications	1. Review the most current System Development Life Cycle
	2. Review additional System Development Life Cycle policies and procedures to ensure security polices and procedures have been incorporated
	3. Perform inquiries of appropriate personnel regarding major systems maintained at the site
	4. Review documentation indicating accreditations and certifications were performed for the noted systems

G. Determine if hiring, transfer, termination and performance policies address security.	1. Review hiring policies and procedure to ensure they address security
	2. Review transfer policies and procedures to ensure they address security
	3. Review termination policies and procedures to ensure they address security
	4. Ensure performance policies and procedures (i.e., Rules of Behavior and Performance Evaluations) to ensure they address security
H. Determine if employee background checks are performed.	1. Review policies and procedures for performing background checks
	2. Select a sample of employees and ensure background investigations have been completed
I. Determine if security employees have adequate security training and expertise.	1. Identify all employees responsible for administering security
	2. Review training records and certifications for all security employees to ensure adequate training has been received
J. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Review policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures
	2. Review documentation indicating management has periodically reviewed, updated, and approved security policies and procedures
K. Determine if management ensures that corrective actions are effectively implemented.	1. Review policies and procedures for ensuring that corrective actions are effectively implemented.
	2. Review evidence that management ensures corrective actions are effectively implemented.
Section IV: Review of Security Awareness Training	
A. Determine if employees have received a copy of the Rules of Behavior.	1. Inquire of the appropriate personnel regarding the maintenance and distribution of the Rules of Behavior for all types of employees
	2. Review the most current version of the Rules of Behavior
	3. Select a sample of employees and ensure they have received a copy of the most current version of the rules of behavior
B. Determine if employee training and professional development has been documented and formally monitored.	1. Inquire of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development
	2. Review policies and procedures regarding the documentation and formal monitoring of employee training and professional development
	3. For a selected sample of employees, review evidence that training and professional development is documented and formally monitored
C. Determine if there is mandatory	1. Review policies and procedures regarding mandatory annual refresher security training

annual refresher training for security.	2. Review the most recent security awareness training curriculum.
	3. For a selected sample of employees, review evidence that all attended the mandatory annual refresher security training
D. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	1. Review policies and procedures regarding methods to make employees aware of security
	2. Conduct a walk through of the site to ensure posters/flyers are in fact hanging in visible areas
	3. Inspect evidence that methods to make employees aware of security are implemented
E. Determine if employees have received a copy of or have easy access to agency security procedures and policies.	1. Inquire of appropriate personnel regarding employee access to agency security procedures and policies
	2. Inspect evidence that employees have received a copy or have easy access to the agency security procedures and policies
	3. Review policies and procedures in which employees have easy access to ensure they are the most current
F. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identify all employees responsible for administering security
	2. Review training records and certifications for all security employees to ensure adequate training has been received
	3. Inquire of appropriate personnel regarding the documentation and tracking of application specific training for employees
	4. Review the most recent application specific training curriculum
	5. Inspect evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked
Section V: Review of periodic testing and evaluation of the effectiveness of IT security policies	
A. Determine if management reports for the review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspect evidence that periodic testing of IT security policies and procedures (including network risk assessments, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted
B. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance	1. Inspect evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA

from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	
C. Determine if remedial action is being taken for issues noted on audits.	1. Review policies and procedures for taking remedial action for issues noted on audits.
	2. Inspect evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored
Section VI: Review of Remedial Activities, processes, and reporting for deficiencies	
A. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Review policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness
	2. Inspect evidence that weaknesses are tracked in a formal database (or other manner)
	3. Inspect evidence that planned actions to address all IT security weaknesses is being tracked
B. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Review policies and procedures for preparing Corrective Action Plans (CAP)
	2. Review all quarterly CAPs that were performed during the scope of the review to ensure corrective actions have been taken to address IT security weaknesses
C. Determine the number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Review policies and procedures for preparing Corrective Action Plans (CAP)
	2. Review all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed
	3. Inspect evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
Section VII: Review of Incident Detection, reporting, and response	
A. Determine that management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.	1. Review policies and procedures for monitoring systems and networks for unusual activity, and or intrusion attempts
	2. Inspect evidence that management is monitoring systems and networks for unusual activity and/or intrusion attempts based on the policies and procedures
B. Determine if management has procedures to take and has taken action in response to unusual activity, intrusion attempts and	1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur
	2. Inspect evidence management has taken action to unusual activity, intrusion attempts, and/or actual intrusions if any have occurred within the scope of the review

actual intrusions.	
C. Determine that management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Ensure policies and procedures are in accordance with FISMA standards
Section VIII: Policies and procedures for continuity of operations and related physical security safeguards for IT systems.	
A. Determine if critical data and operations are formally identified and prioritized.	1. Review the Business Contingency Plan to ensure critical data and operations are formally identified and prioritized
B. Determine if resources supporting critical operations are identified in contingency plans.	1. Review the Business Contingency Plan to ensure resources supporting critical operations are identified.
C. Determine if emergency processing priorities are established.	1. Review emergency processing priorities to ensure they are formally documented
D. Determine if data and program backup procedures have been implemented	1. Review data and program backup policies and procedures
	2. Inspect evidence (i.e., backup logs) that data and program backup procedures have been implemented
E. Determine if adequate environmental controls have been implemented.	1. Inquire of data center manager concerning the environmental controls implemented in the data center
	2. Perform Walkthrough of data center to ensure adequate environmental controls have been implemented
F. Determine if staff have been trained to respond to emergencies	1. Review emergency response policies and procedures
	2. Review emergency response training curriculum
	3. Inspect evidence that emergency response training has been provided for applicable staff
G. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	1. Review hardware maintenance procedures exist to help prevent unexpected interruptions
	2. Review problem management procedures exist to help prevent unexpected interruptions
	3. Review change management procedures exist to help prevent unexpected interruptions
H. Determine if policies and procedures for disposal of data and equipment exist and include	1. Review policies and procedures regarding the disposal of data and equipment to ensure applicable Federal security and privacy requirements are included

applicable Federal security and privacy requirements.	
I. Determine if an up-to-date contingency plan is documented.	1. Inspect evidence that the contingency plan was approved within the scope of the review
J. Determine if arrangements have been made for alternate data processing and telecommunications facilities.	1. Review the contingency plan to ensure arrangements have been made for alternate data processing and telecommunications facilities.
	2. Review the contract with the organization that will provide alternate data processing and telecommunications operations if necessary.
K. Determine if the plan is periodically tested.	1. Review policies and procedures regarding periodically testing the contingency plan
	2. Inspect evidence that the contingency plan has been periodically tested
L. Determine if the results are analyzed and contingency plans adjusted accordingly.	1. Inspect evidence that the contingency plan is adjusted accordingly after the tests are performed and analyzed
M. Determine if physical security controls exist to protect IT resources	1. Inquire of data center manager concerning the physical security controls implemented in the data center
	2. Perform Walkthrough of data center to ensure adequate physical security controls exist

APPENDIX IV: DETAILED SAS 70 TESTING PROCEDURES

Control Activity	Detailed Testing
A.1 An entity-wide security program has been documented, approved and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure and clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness and ensure security officer training and employee security awareness.	
1. A security plan is documented and approved.	1. Reviewed the security plan.
	2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
2. The security plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed, updated and is current.
3. A security management structure has been established.	1. Reviewed the security plan and the entity's organization chart.
	2. Interviewed security management staff.
	3. Reviewed pertinent organization charts and job descriptions.
4. Information security responsibilities are clearly assigned.	1. Reviewed the security plan.
	2. Reviewed the security management's organization chart
	3. Reviewed the security management's formal job descriptions
5. Owners and users are aware of security policies.	1. Reviewed documentation supporting or evaluating the awareness program. Observed a security briefing.
	2. Interviewed data owners and system users. Determined what training they have received and if they are aware of their security-related responsibilities.
	3. Reviewed memos, electronic mail files, or other policy distribution mechanisms.
	4. Reviewed personnel files to test whether security awareness statements are current.
	5. Called selected users, identified yourself as security or network staff, and attempted to talk them into revealing their password.
	6. Reviewed security training schedules
	7. Reviewed security training materials
	8. For a selection of owners and users ensured that they have attended the required trainings
6. Management periodically assesses the appropriateness of security policies and compliance	1. Reviewed the reports resulting from recent assessments, including the most recent FMFIA report.
	2. Determined when last independent review or audit occurred and reviewed results.

with them.	3. Reviewed written authorizations or accreditation statements.
	4. Reviewed documentation related to corrective actions.
	5. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures
	6. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures
7. Employees have adequate training and expertise.	1. Reviewed job descriptions for security management personnel, and for a selection of other personnel.
	2. For a selection of employees, compared personnel records on education and experience with job descriptions.
	3. Reviewed training program documentation.
	4. Reviewed training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
8. Employee training and professional development has been documented and formally monitored.	1. Inquired of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development
	2. Reviewed policies and procedures regarding the documentation and formal monitoring of employee training and professional development
	3. For a selected sample of employees, reviewed evidence that training and professional development is documented and formally monitored
9. There is mandatory annual refresher training for security.	1. Reviewed policies and procedures regarding mandatory annual refresher security training
	2. Reviewed the most recent security awareness training curriculum.
	3. For a selected sample of employees, reviewed evidence that all attended the mandatory annual refresher security training
10. Systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	1. Reviewed policies and procedures regarding methods to make employees aware of security
	2. Conducted a walk through of the site to ensure posters/flyers are in fact hanging in visible areas
	3. Inspected evidence that methods to make employees aware of security are implemented
11. Employees have received a copy of or have easy access to agency security procedures and policies.	1. Inquired of appropriate personnel regarding employee access to agency security procedures and policies
	2. Inspected evidence that employees have received a copy or have easy access to the agency security procedures and policies
	3. Reviewed policies and procedures in which employees have easy access to ensure they are

	the most current
12. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identified all employees responsible for administering security
	2. Reviewed training records and certifications for all security employees to ensure adequate training has been received
	3. Inquired of appropriate personnel regarding the documentation and tracking of application specific training for employees
	4. Reviewed the most recent application specific training curriculum
	5. Inspected evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked
A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual and temporary) and include termination and transfer procedures that require exit interviews, return of property, such as keys and ID cards, notification to security management of terminations, removal of access to systems and escorting of terminated employees out of the facility.	
1. Hiring, transfer, termination, and performance policies address security.	1. Reviewed hiring policies and procedure to ensure they address security
	2. Reviewed transfer policies and procedures to ensure they address security
	3. Reviewed termination policies and procedures to ensure they address security
	4. Ensured performance policies and procedures (ie, Rules of Behavior and Performance Evaluations) address security
	5. Reviewed reinvestigation policies.
	6. Reviewed policies and procedures for performing background checks
	7. For a selection of sensitive positions, inspected personnel records and determined whether background reinvestigations have been performed.
	8. Reviewed policies on confidentiality or security agreements.
	9. For a selection of such users, determined whether confidentiality or security agreements are on file.
	10. Reviewed vacation policies.
	11. Inspected personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	12. Determined who performed vacationing employee's work during vacation.
	13. Reviewed job rotation policies.
	14. Reviewed staff assignment records and determined whether job and shift rotations occur.

	15. Reviewed pertinent policies and procedures.
	16. For a selection of terminated or transferred employees, examined documentation showing compliance with policies.
	17. Compared a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures
3. Employees have received a copy of the Rules of Behavior.	1. Inquired of the appropriate personnel regarding the maintenance and distribution of the Rules of Behavior for all types of employees
	2. Reviewed the most current version of the Rules of Behavior
	3. Selected a sample of employees and ensure they have received a copy of the most current version of the rules of behavior
A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.	
1. Resource classifications and related criteria have been established.	1. Reviewed data classification policies and procedures
	2. Interviewed resource owners.
2. Owners have classified resources.	1. Reviewed resource classification documentation and compared to risk assessments. Discussed any discrepancies with appropriate officials.
3. Data sensitivity and integrity of the data have been documented and if data have been classified.	1. Reviewed evidence based on policies and procedures that data has been classified
A.4 Access to computerized applications, systems software and Medicare data are appropriately authorized, documented and monitored and includes approval by resource owners, procedures to control emergency and temporary access and procedures to share and properly dispose of data.	
1. Resource owners have identified authorized users and their access authorized.	1. Reviewed pertinent written policies and procedures.
	2. For a selection of users (both application user and IS personnel) reviewed access authorization documentation.
	3. Interviewed owners and reviewed supporting documentation. Determined whether

	inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, reviewed authorization and justification.
	5. Interviewed security managers and reviewed documentation provided to them.
	6. Reviewed a selection of recent profile changes and activity logs.
	7. Obtained a list of recently terminated employees from Personnel and, for a selection, determined whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Reviewed pertinent policies and procedures.
	2. Compared a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.
	3. Determined the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examined standard approval forms.
	2. Interviewed data owners.
	3. Examined documents authorizing file sharing and file sharing agreements.
4. Sanitation of equipment and media prior to disposal or reuse.	1. Reviewed written procedures.
	2. Interviewed personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examined documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, tested that they have been appropriately sanitized.
5. Access authorizations are appropriately limited.	1. Reviewed policies and procedures regarding the disposal of data and equipment to ensure applicable Federal security and privacy requirements are included
	2. Interviewed management and systems personnel regarding access restrictions.
	3. Observed personnel accessing system software, such as sensitive utilities, and noted the controls encountered to gain access.
	4. Attempted to access the operating system and other system software.
	5. Selected some systems programmers and determined whether management-approved documentation supports their access to system software.
	6. Selected some application programmers and determined whether they are not authorized access.
	7. Determined the last time the access capabilities of system programmers were reviewed.
6. Passwords, tokens, or other	1. Reviewed pertinent policies and procedures.

devices are used to identify and authenticate users.	2. Reviewed security software password parameters.
	3. Observed users keying in passwords.
	4. Attempted to log on without a valid password; make repeated attempts to guess passwords.
	5. Assessed procedures for generating and communicating passwords to users.
	6. Reviewed a system-generated list of current passwords.
	7. Searched password file using audit software.
	8. Attempted to log on using common vendor supplied passwords.
	9. Interviewed users and security managers.
	10. Reviewed a list of IDs and passwords.
	11. Repeatedly attempted to log on using invalid passwords.
	12. Reviewed security logs.
	13. Reviewed pertinent policies and procedures.
	14. Reviewed documentation of such comparisons.
	15. Interviewed security managers.
	16. Made comparison using audit software.
	17. Viewed dump of password files (e.g., hexadecimal printout).
	18. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor obtained the assistance of a specialist.
7. Identification of access paths.	1. Reviewed access path diagram.
8. Logical controls over data files and software programs.	1. Interviewed security administrators and system users.
	2. Reviewed security software parameters.
	3. Observed terminals in use.
	4. Reviewed a system-generated list of inactive logon IDs, and determined why access for these users has not been terminated.
	5. Determined library names for sensitive or critical files and libraries and obtained security reports of related access rules. Using these reports, determined who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Performed penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system.
	7. When performing outsider tests, tested the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.

	8. When performing insider tests, used an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, tried to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determined whether naming conventions are used.
9. Logical controls over a database.	1. Reviewed pertinent policies and procedures.
	2. Interviewed database administrator.
	3. Reviewed DBMS and DD security parameters.
	4. Tested controls by attempting to access restricted files.
	5. Reviewed security system parameters.
10. Logical controls over telecommunications access.	1. Reviewed pertinent policies and procedures.
	2. Reviewed parameters set by communications software or teleprocessing monitors.
	3. Tested telecommunications controls by attempting to access various files through communications networks.
	4. Identified all dial-up lines through automatic dialer software routines and compared with known dial-up access. Discussed discrepancies with management.
	5. Interviewed telecommunications management staff and users.
	6. Reviewed pertinent policies and procedures.
	7. Viewed the opening screen seen by telecommunication system users.
	8. Reviewed the documentation showing changes to dial-in numbers.
	9. Reviewed entity's telephone directory to verify that the numbers are not listed.
11. Cryptographic tools	1. To evaluate cryptographic tools, the auditor obtained the assistance of a specialist.
A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.	
1. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Tested the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtained a list of vendor-supplied software and determined if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally reviewed the installation of system software components and determined whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Performed an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.

	5. Obtained a list of all system software on test and production libraries used by the entity.
	6. Verified that access control software restricts access to system software.
	7. Using security software reports, determined who has access to system software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated In the presence of the auditor.
	8. Verified that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquired whether disabling has occurred.
	10. Tested for default presence using vendor standard IDs and passwords.
	11. Determined what terminals are set up as master consoles and what controls exist over them.
	12. Tested to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
2. Security policies and procedures include controls to address platform security configurations, and patch management.	1. Reviewed platform security configuration policies and procedures
	2. Reviewed patch management policies and procedures
3. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA
A.6 Physical access by all employees, including visitors, to Medicare facilities, data centers and systems is appropriately authorized, documented, and access violations are monitored and investigated.	
1. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Reviewed a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.
	2. Performed a Walkthrough of data center to ensure adequate physical security controls exist
	3. Reviewed lists of individuals authorized access to sensitive areas and determined the appropriateness for access.
	4. Before becoming recognized as the auditor, attempted to access sensitive areas without

	escort or identification badges.
	5. Observed entries to and exits from facilities during and after normal business hours.
	6. Observed utilities access paths.
	7. Inquired of data center manager concerning the physical security controls implemented in the data center
	8. Observed entries to and exits from sensitive areas during and after normal business hours.
	9. Reviewed procedures for the removal and return of storage media from and to the library.
	10. Selected from the log some returns and withdrawals, verified the physical existence of the tape or other media, and determined whether proper authorization was obtained for the movement.
	11. Observed practices for safeguarding keys and other devices.
	12. Reviewed written emergency procedures.
	13. Examined documentation supporting prior fire drills.
	14. Observed a fire drill.
2. Visitors are controlled.	1. Reviewed visitor entry logs.
	2. Observed entries to and exits from sensitive areas during and after normal business hours.
	3. Interviewed guards at facility entry.
	4. Reviewed documentation on and logs of entry code changes.
	5. Observed appointment and verification procedures for visitors.
3. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security violation reports.
	3. Examined documentation showing reviews of questionable activities.
4. Suspicious access activity is investigated and appropriate action is taken.	1. Tested a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
	2. Interviewed senior management and personnel responsible for summarizing violations.
	3. Reviewed any supporting documentation.
5. Physical security controls exist to protect IT resources.	1. Inquired of data center manager concerning the physical security controls implemented in the data center
	2. Performed Walkthrough of data center to ensure adequate physical security controls exist
6. Physical and logical access controls have been established.	1. Interviewed management and subordinate personnel.
A.7 Medicare application and related systems software development and maintenance activities are authorized, documented,	

tested, and approved.	
1. Authorizations for software modifications are documented and maintained,	1. Identified recent software modifications and determined whether change request forms were used.
	2. Examined a selection of software change request forms for approvals.
	3. Interviewed software development staff.
2. Emergency changes are promptly tested and approved.	1. Reviewed procedures.
	2. For a selection of emergency changes recorded in the emergency change log, reviewed related documentation and approval.
3. System software changes are authorized, tested, and approved before implementation.	1. Reviewed pertinent policies and procedures.
	2. Interviewed management and systems personnel.
	3. Reviewed procedures for identifying and documenting system software problems.
	4. Interviewed management and systems programmers.
	5. Reviewed 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.
	6. Determined what authorizations and documentation are required prior to initiating system software changes.
	7. Selected recent system software changes and determined whether the authorization was obtained and the change is supported by a change request document.
	8. Determined the procedures used to test and approve system software prior to its implementation.
	9. Selected recent system software changes were tested to verify indicated procedures were in fact used.
	10. Reviewed procedures used to control and approve emergency changes.
	11. Selected some emergency changes to system software and tested whether the indicated procedures were in fact used.
4. Installation of system software is documented and reviewed.	1. Interviewed management and systems programmers about scheduling and giving advance notices when system software is installed.
	2. Reviewed recent installations and determine whether scheduling and advance notification did occur.
	3. Determined whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.

	4. Interviewed management, systems programmers, and library control personnel, and determined who migrates approved system software to production libraries and whether outdated versions are removed from production libraries.
	5. Reviewed supporting documentation for some system software migrations and the removal of outdated versions from production libraries.
	6. Interviewed data center management about their role in reviewing system software installations.
	7. Reviewed some recent system software installations and determined whether documentation shows that logging and management review occurred.
	8. Interviewed system software personnel concerning a selection of system software and determined the extent to which the operating version of the system software is currently supported by the vendor.
	9. Interviewed management and systems programmers about the currency of system software and the currency and completeness of software documentation.
	10. Reviewed documentation and tested whether recent changes are incorporated.
5. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Reviewed the most current System Development Life Cycle
	2. Reviewed additional information (ie, System Security Plan) which outline security controls included in the cost of developing new systems
	3. Reviewed software change control policies and procedures to ensure changes are being controlled effectively.
6. Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	1. Performed inquiries of appropriate personnel regarding major systems maintained at the site.
	2. Reviewed documentation indicating accreditations and certifications were performed for the noted systems
	3. Ensured accreditations and certifications are in compliance with FISMA policies
A.8 A System Development Life Cycle methodology is documented and in use and includes planning for and costs for security requirements in systems.	
1. A system development life cycle methodology (SDLC) has been implemented.	1. Reviewed SDLC methodology.
	2. Reviewed system documentation to verify that SDLC methodology was followed.
	3. Interviewed staff.
	4. Reviewed training records.

2. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	1. Reviewed additional information (ie, System Security Plan) which outline security controls included in the cost of developing new systems
	2. Reviewed software change control policies and procedures to ensure changes are being controlled effectively.
3. Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications	1. Reviewed additional System Development Life Cycle policies and procedures to ensure security polices and procedures have been incorporated
	2. Performed inquiries of appropriate personnel regarding major systems maintained at the site.
	3. Reviewed documentation indicating accreditations and certifications were performed for the noted systems
A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.	
1. Authorizations for software modifications are documented and maintained,	1. Identified recent software modifications and determined whether change request forms were used.
	2. Examined a selection of software change request forms for approvals.
	3. Interviewed software development staff.
2. Use of public domain and personal software is restricted.	1. Reviewed pertinent policies and procedures.
	2. Interviewed users and data processing staff.
3. Changes are controlled as programs progress through testing to final approval.	1. Reviewed test plan standards.
	2. For the selected software change requests (1) reviewed specifications; (2) traced changes from code to design specifications; (3) reviewed test plans; (4) compared test documentation with related test plans; (5) analyzed test failures to determine if they indicate ineffective software testing; (6) reviewed test transactions and data.
	3. For the software change requests selected for control activity CC-1.2 (continued): (1) reviewed test results; (2) reviewed documentation of management or security administrator reviews; (3) verified user acceptance; and (4) reviewed updated documentation.
	4. Determined whether operational systems experienced a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
4. Emergency processing priorities are established.	1. Reviewed emergency processing priorities to ensure they are formally documented
5. Data and program backup	1. Reviewed data and program backup policies and procedures

procedures have been implemented	2. Inspected evidence (ie, backup logs) that data and program backup procedures have been implemented
6. Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	1. Reviewed hardware maintenance procedures that exist to help prevent unexpected interruptions
	2. Reviewed problem management procedures that exist to help prevent unexpected interruptions
	3. Reviewed change management procedures that exist to help prevent unexpected interruptions
A.10 Access to program libraries is properly restricted and movement of programs among libraries is controlled.	
1. Programs are labeled and inventoried.	1. Reviewed pertinent policies and procedures.
	2. Interviewed personnel responsible for library control.
	3. Examined a selection of programs maintained in the library and assessed compliance with prescribed procedures.
	4. Determined how many prior versions of software modules are maintained.
2. Access to program libraries is restricted.	1. Examined libraries in use.
	2. Interviewed library control personnel.
	3. Verified that source code exists for a selection of production load modules.
	4. For critical software production programs, determined whether access control software rules are clearly defined.
	5. Tested access to program libraries by examining security system parameters.
	6. Selected some program tapes from the log and verified the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
3. Movement of programs and data among libraries is controlled.	1. Reviewed pertinent policies and procedures.
	2. For a selection of program changes, examined related documentation to verify that: (1) procedures for authorizing movement among libraries were followed, and (2) before and after images were compared.
A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.	
1. Incompatible duties have been identified and policies implemented to segregate these duties.	1. Reviewed pertinent policies and procedures.
	2. Interviewed selected management and IS personnel regarding segregation of duties.
	3. Reviewed an agency organization chart showing IS functions and assigned personnel.
	4. Interviewed selected personnel and determined whether functions are appropriately

	segregated.
	5. Determined whether the chart is current and each function is staffed by different individuals.
	6. Reviewed relevant alternate or backup assignments and determined whether the proper segregation of duties is maintained.
	7. Observed activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	8. Reviewed the organizational chart and interviewed personnel to determine that assignments do not result in a single person being responsible for the indicated combination of functions.
	9. Determined through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	10. Reviewed the adequacy of documented operating procedures for the data center.
2. Job descriptions have been documented.	1. Reviewed job descriptions for several positions in organizational units and for user security administrators.
	2. Determined whether duties are clearly described and prohibited activities are addressed.
	3. Reviewed the effective dates of the position descriptions and determined whether they are current.
	4. Compared these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	5. Reviewed job descriptions and interviewed management personnel.
3. Employees understand their duties and responsibilities.	1. Interviewed personnel filling positions for the selected job descriptions (see above). Determined if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	2. Determined from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	3. Interviewed management personnel in these activities.
4. Management reviews effectiveness of control techniques.	1. Interviewed management and subordinate personnel.
	2. Selected documents or actions that require supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	3. Determined which reviews are conducted to assess the adequacy of duty segregation. Obtained and reviewed results of such reviews.

5. Formal procedures guide personnel in performing their duties.	1. Reviewed manuals.
	2. Interviewed supervisors and personnel.
	3. Observed processing activities.
6. Active supervision and review are provided for all personnel.	1. Interviewed supervisors and personnel.
	2. Observed processing activities.
	3. Reviewed history log reports for signatures indicating supervisory review.
	4. Determined who is authorized to perform the initial program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determined whether operators override the IPL parameters.
A.12 Activities of employees should be controlled via formal operating procedures that include monitoring of employee activities by management with documentation maintained to provide evidence of management's monitoring and review process.	
1. Audit trails are maintained.	1. Reviewed security software settings to identify types of activity logged.
2. Actual or attempted unauthorized, unusual, or sensitive access is monitored.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security violation reports.
	3. Examined documentation showing reviews of questionable activities.
3. Policies and techniques have been implemented for using and monitoring use of system utilities.	1. Reviewed pertinent policies and procedures.
	2. Interviewed management and systems personnel regarding their responsibilities.
	3. Determined whether logging occurs and what information is logged.
	4. Reviewed logs.
	5. Using security software reports, determined who can access the logging files.
4. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interviewed technical management regarding their reviews of privileged system software and utilities usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel regarding these investigations.
	4. Reviewed documentation supporting these investigations.
	5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interviewed management and analyzed their reviews concerning the use of system software.

	8. Determined what management reviews have been conducted, and their currency, over this area.
5. Formal procedures guide personnel in performing their duties.	1. Reviewed manuals.
	2. Interviewed supervisors and personnel.
	3. Observed processing activities.
6. Active supervision and review are provided for all personnel.	1. Interviewed supervisors and personnel.
	2. Observed processing activities.
	3. Reviewed history log reports for signatures indicating supervisory review.
A.13 A regular risk assessment of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.	
1. Risks are periodically assessed.	1. Reviewed risk assessment policies.
	2. Reviewed the most recent high-level risk assessment.
	3. Reviewed the objectivity of personnel who performed and reviewed the assessment.
2. The current system configuration is documented, including links to other systems.	1. Reviewed the most recent system configuration
	2. Reviewed the system configuration and/or related documentation indicating it has been reviewed and kept current
3. Data sensitivity and integrity of the data have been documented and if data have been classified.	1. Reviewed data classification policies and procedures
	2. Reviewed evidence based on policies and procedures that data has been classified
4. Threat sources, both natural and manmade, have been formally identified	1. Reviewed risk assessment to ensure threat sources, both natural and man-made, have been identified and documented
5. A list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.	1. Reviewed the risk assessment to ensure a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed.
	2. Reviewed the risk assessment and/or related documentation indicating it has been reviewed and kept current
6. An analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.	1. Reviewed the risk assessment to ensure mitigating controls are documented.
	2. Reviewed the risk assessment to ensure mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities

7. Final risk determinations and related management approvals have been documented and maintained on file.	1. Reviewed the risk assessment to ensure final risk determinations are documented
	2. Reviewed risk assessment and/or related documentation indicating it has been approved (currently)
8. A mission/business impact analysis have been conducted and documented.	1. Reviewed documented critical business processes
	2. Reviewed mission/business impact analysis to ensure it has been documented for the critical business processes
9. Obtain management's list of additional controls that have been identified to mitigate identified risks.	1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
10. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.	1. Performed inquiries of appropriate personnel regarding systems for which controls have been tested
	2. Reviewed evidence (ie, internal/external audits) indicating system controls have been tested and evaluated for the identified systems
	3. Reviewed evidence (ie, internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits
	4. Ensured all reviews have been performed within the scope of the review
A.14 A centralized risk management focal point for IT risk assessment has been established that includes promotion awareness programs, processes and procedures to mitigate risks and monitoring processes to assess the effectiveness of risk mitigation programs.	
1. A security management structure has been established.	1. Reviewed the security plan and the entity's organization chart.
	2. Interviewed security management staff.
	3. Reviewed pertinent organization charts and job descriptions.
	4. Interviewed the security manager.
2. Information security responsibilities are clearly assigned.	1. Reviewed the security plan.
3. Final risk determinations and related management approvals have been documented and maintained on file.	1. Reviewed the risk assessment to ensure final risk determinations are documented
	2. Reviewed risk assessment and/or related documentation indicating it has been approved (currently)
4. Obtain management's list of additional controls that have been	1. Reviewed any additional documented lists of controls identified to mitigate identified risks.

identified to mitigate identified risks.	
5. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	1. Reviewed the most current risk assessment
	2. Reviewed IT Security policies and procedures to ensure they reduce the risk outlined in the risk assessment
	3. Ensured IT Security policies and procedures are current
6. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures
7. Management reports for the review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspected evidence that periodic testing of IT security policies and procedures (including network risk assessments, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted
8. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA
A.15 A risk assessment and systems security plan has been documented, approved, and monitored by management in accordance with the CMS Risk Assessment and Systems Security Plan Methodologies.	
1. Risks are periodically assessed.	1. Reviewed risk assessment policies.
	2. Reviewed the most recent high-level risk assessment.

	3. Reviewed the objectivity of personnel who performed and reviewed the assessment.
2. A security plan is documented and approved.	1. Reviewed the security plan.
	2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
3. The plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed and updated and is current.
A.16 Regularly scheduled processes required to support the Medicare Contractor's continuity of operations (data, facilities or equipment) are performed.	
1. Data and program backup procedures have been implemented.	1. Reviewed written policies and procedures for backing up files.
	2. Compared inventory records with the files maintained off-site and determined the age of these files.
	3. For a selection of critical files, located and examined the backup files. Verified that backup files can be used to recreate current reports.
	4. Determined whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	5. Located and examined documentation.
	6. Examined the backup storage site.
2. Adequate environmental controls have been implemented.	1. Examined the entity's facilities
	2. Interviewed site managers.
	3. Observed that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observed the operation, location, maintenance and access to the air cooling system.
	5. Observed whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determined whether the activation of heat and smoke detectors will notify the fire department.
3. Staff have been trained to respond to emergencies.	1. Interviewed data center staff.
	2. Reviewed training records.
	3. Reviewed training course documentation.
	4. Reviewed emergency response procedures.
	5. Reviewed test policies.
	6. Reviewed test documentation.

	7. Interviewed data center staff.
4. Effective hardware maintenance, problem management, and change management procedures exist.	1. Reviewed hardware maintenance procedures.
	2. Reviewed problem management procedures.
	3. Reviewed change management procedures.
A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components and operations.	
1. Management ensures that corrective actions are effectively implemented.	1. Reviewed the status of prior-year audit recommendations and determined if implemented corrective actions have been tested.
	2. Reviewed recent FMFIA reports.
	3. Reviewed policies and procedures for ensuring that corrective actions are effectively implemented.
	4. Reviewed evidence that management ensures corrective actions are effectively implemented.
2. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Reviewed the most recent CMS CSR
	2. Noted GAPs in compliance as documented in the CMS CSR
	3. Reviewed management's response to the CSR to ensure proper controls are in place/are in the process of being in place
3. Weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Reviewed policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness
	2. Inspected evidence that weaknesses are tracked in a formal database (or other manner)
	3. Inspected evidence that planned actions to address all IT security weaknesses are being tracked
4. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Reviewed policies and procedures for preparing Corrective Action Plans (CAP)
	2. Reviewed all quarterly CAPs that were performed during the scope of the review to ensure corrective actions have been taken to address IT security weaknesses
5. The number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Reviewed policies and procedures for preparing Corrective Action Plans (CAP)
	2. Reviewed all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed
	3. Inspected evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.

6. Remedial action is being taken for issues noted on audits.	1. Reviewed policies and procedures for taking remedial action for issues noted on audits.
	2. Inspected evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored
A.18 Management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.	
1. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.
	2. Review documentation supporting incident handling activities.
	3. Determine qualifications of response team members.
2. Audit trails are maintained.	1. Review security software settings to identify types of activity logged.
A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts and actual intrusions.	
1. Suspicious access activity is investigated and appropriate action is taken.	1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Tested a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
	3. Interviewed senior management and personnel responsible for summarizing violations.
	4. Reviewed any supporting documentation.
	5. Reviewed policies and procedures and interviewed appropriate personnel.
	6. Reviewed any supporting documentation.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interviewed technical management regarding their reviews of privileged system software and utilities usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel regarding these investigations.
	4. Reviewed documentation supporting these investigations.
	5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interviewed management and analyzed their reviews concerning the use of system software.
	8. Determined what management reviews have been conducted, and their currency, over this area.
A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the	

Federal Information Security Management Act (FISMA)	
1. Management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.
	2. Ensured policies and procedures are in accordance with FISMA standards

APPENDIX V: STIG CHECKLIST

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.
	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.

System Type	Standards and Checklists Available	Comments
Windows 2003 Windows XP Windows 2000 Windows NT 4.0 SQL Server IIS	http://www.microsoft.com/technet/Security/default.mspx 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	http://csrc.nist.gov/pcig/STIGs/WindowsXP.doc http://csrc.nist.gov/pcig/CHECKLISTS/winxp-checklist-062504.zip	DISA Windows XP Security Technical Implementation Guide (STIG). 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.
	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.

System Type	Standards and Checklists Available	Comments
	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	http://csrc.nist.gov/pcig/STIGs/os390-lparstig-v2r1-jul03.doc http://csrc.nist.gov/pcig/CHECKLISTS/lpar-checklist-2v103-062504.doc http://csrc.nist.gov/pcig/STIGs/OS-390V5R0-Vol1.zip http://csrc.nist.gov/pcig/STIGs/OS-390V5R0-Vol2.zip http://csrc.nist.gov/pcig/CHECKLISTS/OS390-racf-checklist-v4r13.doc http://csrc.nist.gov/pcig/CHECKLISTS/OS390-acf2-checklist-v4r13.doc http://csrc.nist.gov/pcig/CHECKLISTS/os390-tss-checklist-v4r13.doc	DISA OS/390 Logical Partition STIG DISA OS/390 Logical Partition Checklist DISA OS/390 MVS STIG Volume 1 DISA OS/390 MVS STIG Volume 2 DISA OS/390 RACF Checklist DISA OS/390 ACF2 Checklist DISA OS/390 TSS Checklist
VMS VAX	http://csrc.nist.gov/pcig/CHECKLISTS/vms-openvs-srrchklst-v2r11.zip	DISA VMS VAX Checklist
Wireless security	http://csrc.nist.gov/pcig/STIGs/Wireless-STIG-V3R1.zip http://csrc.nist.gov/pcig/CHECKLISTS/wireless-chklstv2r11-073003.doc	DISA Wireless STIG DISA Wireless Checklist