Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepaper:

Audits

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *AUDITS*, VERSION 2.0

1) Document title and cover page graphics changed from “CMS Guidebook for Audits” to “CMS Security Whitepaper: Audits”.
2) Deleted section entitled “Executive Summary And Introduction” that preceded the table of contents.
3) Corrected grammar throughout the document.
4) Renumbered document to adhere to current numbering style and updated references within the document.
5) The terms “information technology” and “IT” were changed to “information system” in all FISCAM and CFO audit sections.
6) Removed all material specific to FY 2004.
7) Added new “Executive Summary” section (1).
8) Added new “FISCAM” section (2).
9) Old section I “CFO/EDP Audit Acts” changed to section 3 “CFO/EDP Audits” and replaced with new material.
10) Old section I – Subsection “Site Selection Criteria” was renumbered to section 3.1. Last sentence added.
11) Old section I – Subsection “Audit Steps and Objectives” renumbered to 3.2 and completely replaced.
12) Old section I – Subsection “Testing Procedures” was renumbered to section 3.3 and completely replaced.
13) Old section I – Subsection “Documentation” was renumbered to section 3.4 and completely replaced.
14) Old section I – Subsection “Interviews Required” was renumbered to section 3.5 and completely replaced.
15) Old section I – Subsection “Space and Equipment Requirements” was renumbered to section 3.5 and introductory sentence was added.
16) Old section II “Section 912 Evaluation” renumbered to 4. All subsections renumbered accordingly.
17) Old section III “SAS 70 Audits” renumbered to 5. FISMA Note added.
18) New section 5.2:
    a) updated the list of key FISCAM areas
    b) Corrected A.4 to read “Access to significant computerized applications (such as claims processing), accounting systems, …” by inserting “significant” and “(such as claims processing), accounting systems,”
    c) Corrected A.7 – added last sentence.
19) Old Section IV “Penetration/EVA” changed to 6. Removed FISCAM references from first paragraph.
20) Deleted “Appendix I: Synopsis Of Documentation Required” and “Appendix II: Detailed CFO Testing Procedures”
21) Added “Appendix I: CFO General Controls Testing Procedures” and “Appendix II: CFO Business Process Application Level Controls Testing Procedures”.
22) Updated Appendix IV text of items A4 and A7 to match the updates made to section 5.2.

SUMMARY OF CHANGES IN *AUDITS*, VERSION 1.0

1) Baseline Version 1.0.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

This whitepaper is an update to a guide that was developed to aid contractors, maintainers, and data centers in understanding and preparing for the various types of audits and reviews, which may be performed at their locations. Its purpose is to provide additional information on: audit steps and objectives, documentation requirements, the types of employees that will need to be interviewed, space and equipment requirements for Chief Financial Officer (CFO), Section 912 Reviews, Statement on Auditing Standards (SAS) No. 70 type II audits, and Penetration/External Vulnerability Assessment (EVA) testing.

This whitepaper contains updates that reflect the following documents:

- February 2009 Federal Information Systems Controls Audit Manual (FISCAM). Additional information is contained in FISCAM. The reader should obtain a copy of FISCAM directly from http://www.gao.gov/special.pubs/fiscam.html.

- October 2007 Medicare Financial Management Manual (Rev. 132, 10-05-07)

1.1 FISCAM

As the Federal Information Systems Controls Audit Manual (FISCAM) is central to many audits, providing a methodology for performing information system control audits, additional FISCAM related information is provided. FISCAM is a recognized methodology that can be used for:

- CFO audits (information system controls audit portion),

- EDP audits and information system controls audits, and

- SAS 70 audits.

- also, at the discretion of the auditor, FISCAM may be applied on other than Generally Accepted Government Auditing Standards (GAGAS) audits.

The February 2009 FISCAM has significant revisions that reflect changes in (1) technology used by government entities, (2) audit guidance and control criteria issued by the National Institute of Standards and Technology (NIST), and (3) GAGAS. It provides a methodology for performing information system control audits in accordance with GAGAS. Information system controls consist of those internal controls that are dependent on information systems processing and include general controls and business process application level controls.

Technological evolution is recognized in both the structure and depth of FISCAM audit specifications and more generally in the change from “installation level” general controls to “system level” general controls to reflect the logically networked structure of today’s systems.

Using FISCAM, auditors identify control techniques and determine the effectiveness of controls at each of the following levels:

- Entitywide or component level (general controls) Controls at the entity or component level consist of the entitywide or component wide processes designed to achieve the control activities. They are focused on how the entity or component manages IS related to each general control activity.

- System level (general controls). Controls at the system level consist of processes for managing specific system resources related to either a general support system or major application. These controls are more specific than those at the entity or component level and generally relate to a single type of technology. Within the system level are three further levels that the auditor assesses: network, operating system, and infrastructure application. The three sublevels can be defined as follows:

    - Network. A network is an interconnected or intersecting configuration or system of components.

    - Operating system. An operating system is software that controls the execution of computer programs and may provide various services.

    - Infrastructure applications. Infrastructure applications are software that is used to assist in performing systems operations, including management of network devices. These applications include databases, e-mail, browsers, plug-ins, utilities, and applications not directly related to business processes.

- Business process application level. Controls at the business process application level consist of policies and procedures for controlling specific business processes.

1.2 CFO/EDP AND INFORMATION SYSTEM CONTROL AUDITS

The purpose of these audits is to ensure that proper information system controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IS control is needed from each contractor 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.

The Chief Financial Officer’s Act of 1990 was enacted to improve the general and financial management of the Federal government and established the foundation for the Government Performance Results Act (GPRA). A CFO Act audit is conducted under the guidelines and supervision of the U.S. General Accountability Office (GAO) in accordance the methodology for

performing financial statement audits that is presented in the GAO/Presidents Council on Integrity and Efficiency (PCIE) Financial Audit Manual (FAM). Part of this audit is the assessment of information system controls which is the GAO requires follow the Federal Information Systems Control and Audit Manual (FISCAM). FISCAM defines two (2) control levels: general controls and business process application level controls. Together, these include a total of nine (9) control categories: Security Management, Access Controls, Configuration Management, Segregation of Duties, Contingency Planning, Application Level General Controls (also called Application Security), Business Process Controls, Interface Controls, and Data Management System Controls.

1.3 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 (IS) programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors shall be in compliance with the eight statutory requirements (see below) set forth in the Federal Information Security Management Act (FISMA).

These evaluations are conducted according to procedures established by the Office of Information Services (OIS) with input from the U.S. Department of Health and Human Services (DHHS), Office of Inspector General (OIG). The procedures are organized using the eight FISMA statutory areas which include:

1) Periodic IS Risk Assessments (RA);
2) Policies and procedures based on IS RAs that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the Systems Development Life Cycle (SDLC) and complies with the National Institute of Standards and Technology (NIST) standards;
3) System Security Plans (SSP);
4) Security awareness training;
5) Periodic testing and evaluation of the effectiveness of information system security policies and procedures, including network assessments and penetration activities;
6) Remedial activities, processes and reporting for deficiencies;
7) Incident detection, reporting and response; and
8) Continuity of operations for IT systems.

1.4 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 systems and related processes.

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

1.5 PENETRATION/EVA

Network vulnerability assessments and penetration testing of information systems are required by CMS (see CMSR RA-5: Vulnerability Scanning). A network vulnerability assessment is the systematic examination of an information system to:

- Determine the adequacy of security measures,
- Identify security deficiencies,
- Provide data from which to predict the effectiveness of proposed security measures, and
- Confirm the adequacy of such measures after implementation.

Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization’s security incident response capability.

2 FISCAM

FISCAM is structured hierarchically, defining control levels that have subordinate control categories, each containing critical elements to be evaluated. The evaluation is accomplished by performing control activities which consist of one or more control techniques that are accomplished through assessment procedures. Sometimes, multiple control techniques can be accomplished from the same set of assessment procedures.

It is consistent with NIST and OMB, and considers new IS risks and audit experience. While it includes references/mappings of each critical element to such guidance, additional references have been added to complete consistency with CMS’ CMSRs.

Note that:

- The identification schemes used in FISCAM, NIST SP 800-53, and CMSRs is similar. Within NIST and CMSRs, a matching identifier refers to the same thing (e.g., AC-1 means Access Control Policy and Procedures). A FISCAM identifier is not the same thing (e.g.,

AC-1 means "Adequately protect information system boundaries."). Similarity of identifiers between FISCAM and security control sets means nothing!

- FISCAM evaluations look at information system controls in the context of a system of controls that, when taken together, meet a control objective, called a critical element, and are consequently independent of security control sets. It is not uncommon to see many security controls mapped to a critical element. Specific security controls may also map to multiple critical elements.

- The auditor is responsible for identifying relevant IS control-related criteria issued after December 2008 and, where appropriate, criteria beyond that referred to in the FISCAM. Future updates to the FISCAM, including any implementation tools and related materials, will be posted to the FISCAM website at hyperlink, http://www.gao.gov/special.pubs/fiscam.html.

2.1 CONTROL LEVELS

The two control levels defined in FISCAM are:

- **General Controls** are applicable to the entitywide and system levels, These are the policies, procedures, and other controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. The effectiveness of general controls, which are applicable at the entitywide and system levels, is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the entity and system levels, business process controls generally can be rendered ineffective by circumvention or modification.

- **Business Process Application Level Controls** include the general controls applied at the business process application level (also referred to as application security) as well as the three categories of business process application controls. These are those controls over the completeness, accuracy, validity, confidentiality and availability of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of entitywide and system level general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data that can circumvent or impair the effectiveness of application level controls.

Typically, general controls are evaluated first. If a significant weakness is found, it will result in weaknesses in business process application level controls as well.

Because systems are networked, it is not unusual for weaknesses found in one entity's, or location's, controls to adversely affect other entities and locations. This is especially significant for data centers where a single weakness at the general controls level can result in multiple applications (systems) having significant weaknesses.

2.1 CONTROL CATEGORIES

The control categories of the general controls level are:

- **Security Management (SM)** addresses the entitywide information security management program.

- **Access Controls (AC)** limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls.

- **Configuration Management (CM)** involve the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle.

- **Segregation of Duties (SD)** ensures work responsibilities are divided so that one individual does not control all critical stages of a process.

- **Contingency Planning (CP)** addresses the entity's ability to accomplish its mission after loss of the capability to process, retrieve, or protect electronically maintained information.

The control categories of the business process application level controls level are:

- **Application Level General Controls (AS)**, also referred to as "application security", are general controls operating at the application level (as opposed to entitywide or systemwide), including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.

- **Business Process Controls (BP)** are the automated and/or manual controls applied to business transaction flows and relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing.

- **Interface Controls (IN)** consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion.

- **Data Management System Controls (DA)** consists of the controls and business rules for database management systems, middleware, cryptography, data warehouse, and data reporting/data extraction software.

2.2 OTHER FISCAM HIERARCHY COMPONENTS

Other components within the FISCAM hierarchy are presented, accompanied by mappings to related CMSRs, as follows:

- Critical Elements are presented in section 3 CFO/EDP Audits.
- Control activities, control techniques, and assessment procedures are presented in Appendix I and Appendix II.

3 CFO/EDP AUDITS

A CFO Act audit is conducted under the guidelines and supervision of the U.S. GAO. The GAO requires that all such audits follow FISCAM. This whitepaper contains updates that reflect the February 2009 FISCAM. The reader is encouraged to obtain a copy of FISCAM directly from http://www.gao.gov/special.pubs/fiscam.html.

The purpose of these audits is to ensure that proper IS control exists within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IS control is needed from each contractor site to determine the sufficiency of overall controls for CMS. The control levels are risk based and used to assess the impact of their presence on the financial statements and operations of CMS.

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

3.1 SITE SELECTION CRITERIA

Selection of sites to be included in the CFO Act audit is primarily based on the volume of claims processed, prior findings, and significance of processing done. Smaller sites are rotated into the testing to ensure that their controls are also understood, but such sites are not likely to be audited every year. Because of the new requirements of the security evaluations set forth in Section 912 of the MMA (see section 2.2 of this guide for more detail), the need to rotate smaller sites into testing samples may diminish in the future.

Also, the networked nature of current systems is expected to influence site selection starting in 2009.

3.1 AUDIT STEPS AND OBJECTIVES

This section contains FISCAM Critical Elements and the CMS Security Requirements (CMSR) that relate to each Critical Element. Each base CMSR may have enhancements and associated standards that are required. For example, AC-2 (Account Management) has four (4) enhancements: AC-2(1), AC-2(2), AC-2(3), and AC-2(4), at the high impact level, and six (6) standards AC-2.Std.1 through AC-2-Std-6. When AC-2 is designated as a related control all required enhancements and standards of AC-2 are implicitly included.

Also, some FISCAM audit assessment procedures cross reference others. A FISCAM note is used to highlight these when they refer to other Critical Elements

3.1.1 FISCAM GENERAL CONTROLS – CRITICAL ELEMEMTS

3.1.1.1 SECURITY MANAGEMENT (SM)

SM-1. Establish a security management program.
CMSR: AC-1, AT-1, AU-1, CA-1, CA-3, CM-1, CM-8, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PL-3, PL-6, PS-1, PS-CMS-2, RA-1, SA-1, SA-2, SC-1, SI-1

SM-2. Periodically assess and validate risks.
CMSR: CA-4, CA-6, RA-1, RA-2, RA-3, RA-4

SM-3. Document and implement security control policies and procedures.
CMSR: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1

SM-4. Implement effective security awareness and other security-related personnel policies.
CMSR: AC-2, AT-2, AT-3, AT-4, PE-3, PL-4, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8

SM-5. Monitor the effectiveness of the security program.
CMSR: AU-6, CA-2, CA-4, CA-5, CA-6, CA-7, CM-4, IR-5, PE-6, PL-5, RA-5, SA-11, SI-4, SI-5

SM-6. Effectively remediate information security weaknesses.
CMSR: CA-5

SM-7. Ensure that activities performed by external third parties are adequately secure.
CMSR: AC-20, AT-1, MA-4, MA-5, PS-3, PS-7, SA-4, SA-9
FISCAM note: Coordinate assessment of security awareness training with SM-4.

3.1.1.1 ACCESS CONTROLS (AC)

AC-1. Adequately protect information system boundaries.
CMSR: AC-4, AC-8, AC-9, AC-11, AC-12, AC-17, AC-18, AC-19, CA-3, IA-3, SC-7, SC-10, SC-CMS-6

AC-2. Implement effective identification and authentication mechanisms.
CMSR: AC-2, AC-7, AC-10, AC-14, AU-10, IA-2, IA-3, IA-4, IA-5, IA-6, SA-3, SC-14, SC-17, SC-20, SC-21, SC-22, SC-23

AC-3. Implement effective authorization controls.
CMSR: AC-2, AC-3, AC-6, AC-13, AC-14, AU-2, AU-6, CM-6, CM-7, IA-4, SC-6, SC-14, SC-15

AC-4. Adequately protect sensitive system resources.
CMSR: AC-1, AC-2, AC-3, AC-6, AC-15, AC-16, AC-17, AC-18, AU-2, AU-6, CM-5, IA-4, IA-7, MA-3, MA-4, MP-2, MP-3, MP-4, MP-5, MP-6, SC-2, SC-3, SC-4, SC-8, SC-9, SC-11, SC-12, SC-13, SC-16, SC-18, SC-CMS-3, SC-CMS-4, SI-7

AC-5. Implement an effective audit and monitoring capability.
CMSR: AC-13, AT-5, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, PE-6, PS-8, SC-5, SI-4, SI-5, SI-6

AC-6. Establish adequate physical security controls.
CMSR: AT-1, AT-2, CA-2, MA-1, MA-2, MP-1, MP-2, MP-4, MP-CMS-1, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8, PE-9, PE-11, PE-12, PE-14, PE-15, PE-16, PE-18, PS-3, PS-6, PS-7, RA-3
FISCAM note: Coordinate with FISCAM sections SM-2, SM-3, SM-5, AC-5, SD-1, and CP-2.

3.1.1.2 CONFIGURATION MANAGEMENT (CM)

CM-1. Develop and document CM policies, plans, and procedures.
CMSR: CM-1, SA-3

CM-2. Maintain current configuration identification information.
CMSR: CM-2, CM-6, CM-8, SA-5

CM-3. Properly authorize, test, approve, track and control all configuration changes.
CMSR: AC-3, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-10, SA-11

CM-4. Routinely monitor the configuration.
CMSR: CM-4, CM-5, SA-10, SI-6, SI-7

CM-5. Update software on a timely basis to protect against known vulnerabilities.
CMSR: CM-2, CM-3, MA-1, PL-3, RA-4, RA-5, SA-6, SA-7, SC-1, SC-19, SI-2, SI-3, SI-5, SI-8

CM-6. Appropriately document and approve emergency changes to the configuration.
CMSR: CM-3, SA-10

3.1.1.3 SEGREGATION OF DUTIES (SD)

SD-1. Segregate incompatible duties and establish related policies.
CMSR: AC-5, AC-13, PE-3, PS-2, PS-6, PS-7, SA-2, SA-5
FISCAM note: Perform in conjunction with select SD-2 procedures. Use AC-3 procedures to validate logical enforcement of separation of duties.

SD-2. Control personnel activities through formal operating procedures, supervision, and review.
CMSR: AC-2, AC-5, AC-13, CM-2, PS-1, PS-2, PS-6, PS-8, PS-CMS-1, RA-4, SA-5
FISCAM note: Performed specified step in conjunction with audit steps in critical elements SM-2 and SM-5.

3.1.1.4 CONTINGENCY PLANNING (CP)

CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources.
CMSR: CP-1, CP-2, PL-2, RA-2, RA-3

CP-2. Take steps to prevent and minimize potential damage and interruption.
CMSR: CM-1, CM-3, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, IR-1, MA-1, MA-2, MA-3, MA-5, MA-6, PE-1, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-17, PE-18, PL-2, PL-4, RA-3, SA-5, SA-10, SI-1
FISCAM note: Perform in conjunction with Section AC-6 regarding physical access controls.

CP-3. Develop and document a comprehensive contingency plan.
CMSR: CP-1, CP-2, CP-5, CP-6, CP-7, CP-8, CP-10, SA-3
FISCAM note: Performed in conjunction with Section AC-3 and AC-6 regarding access controls.

CP-4. Periodically test the contingency plan and adjust it as appropriate.
CMSR: CP-4, CP-5, CP-10

3.1.2 FISCAM BUSINESS PROCESS APPLICATION LEVEL CONTROLS – CRITICAL ELEMEMTS

3.1.2.1 APPLICATION LEVEL GENERAL CONTROLS (AS)

AS-1. Implement effective application security management.
CMSR: AC-1, AC-3, AC-5, AT-1, AT-3, AT-4, AU-1, CA-1, CA-2, CA-4, CA-5, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PL-3, PS-1, PS-6, PS-7, RA-1, RA-3, RA-4, SA-1, SA-4, SA-5, SA-9, SA-10, SA-11, SC-1, SI-1
FISCAM note: See all SM (3.2.1.1) controls for other related controls.

AS-2. Implement effective application access controls.
CMSR: AC-2, AC-3, AC-5, AC-6, AC-10, AC-11, AC-12, AC-14, AU-1, AU-2, AU-3, AU-6, IA-2, IA-4, IA-5, PE-1, PL-2, SA-5, SC-2, SC-7, SC-10, SC-17
FISCAM note: See all AC (3.2.1.2) controls for other related controls and refer to AC-2 for more information on criteria for evaluating password policies.

AS-3. Implement effective application configuration management.
CMSR: AC-3, AC-5, AC-6, CA-2, CM-3, CM-4, CM-5, CM-6, SA-3, SA-5, SA-10, SA-11, SI-2, SI-5
FISCAM note: See all CM (3.2.1.3) controls for other related controls.

AS-4. Segregate application user access to conflicting transactions and activities and monitor segregation.
CMSR: AC-2, AC-3, AC-5, AC-13, SA-5
FISCAM note: See all SD (3.2.1.4) controls for other related controls.: Also, the sample of users selected in AS-2 can be used when evaluating AS-4.

AS-5. Implement effective application contingency planning.
CMSR: CP-1, CP-2, CP-4, CP-5, CP-6, CP-9, RA-3, SA-3, SA-5
FISCAM note: See all CP (3.2.1.5) controls for other related controls.

3.1.2.1 BUSINESS PROCESS CONTROLS (BP)

BP-1. Transaction data input is complete, accurate, valid, and confidential.
CMSR: SA-3, SA-5, SI-1, SI-9, SI-10, SI-11
FISCAM note: Coordinate with AS-2 Also note: certain audit procedures apply only to the current environment at the time of test. Supplemental audit procedures would need to be applied at other points during the year to obtain evidence that the control was operating effectively.

BP-2. Transaction data processing is complete, accurate, valid, and confidential.
CMSR: AC-3, AC-4, CM-3, SA-3, SA-5, SA-8, SA-10, SC-9, SI-1, SI-9, SI-10, SI-11, SI-12
FISCAM note: Coordinate with AS-2.

BP-3. Transaction data output is complete, accurate, valid, and confidential.
CMSR: AC-2, MP-2, SA-3, SA-5, SI-1, SI-9, SI-10, SI-11, SI-12

BP-4. Master data setup and maintenance is adequately controlled.
CMSR: AC-3, AC-4, AC-5, SA-3, SA-5, SA-8, SA-10, SC-9, SI-1, SI-9, SI-10, SI-11
FISCAM note: Coordinate with AS-2.

3.1.2.2 INTERFACE CONTROLS (IN)

IN-1. Implement an effective interface strategy and design.
CMSR: SA-3, SA-5, SI-9, SI-10, SI-11

IN-2. Implement effective interface processing procedures.
CMSR: AC-3, SA-2, SA-5, SI-9, SI-10, SI-11

3.1.2.3 DATA MANAGEMENT SYSTEM CONTROLS (DA)

DA-1. Implement an effective data management system strategy and design.
CMSR: AC-3, AC-4, AU-2, AU-3, AU-5, AU-6, SA-3, SA-5, SA-10, SC-2, SI-4, SI-5

3.2 TESTING PROCEDURES

Refer to Appendix I for detailed General Controls testing procedures and Appendix II for detailed Business Process Application Level Controls testing procedures. These can also be used as a benchmark to determine specific changes of future revisions to FISCAM. The current FISCAM can be obtained at http://www.gao.gov/special.pubs/fiscam.html.

3.3 DOCUMENTATION

Documentation needed during phases of the IS control portion of a CFO Act audit usually depends on the contractor's role in the Medicare system and the division of audit task labor between the DHHS OIG and the contract auditor. However, in total it will be consistent with FISCAM, which is presented in this section.

There are some globally applicable items that are either: called for, in total or in part, numerous times during the audit; or of high value in terms of simplifying the audit process. These are presented first, followed by the General Controls and the Business Process Application Level Controls categories.

There are numerous references to policies and procedures in this list. When a reference is to all of the policies, procedures and controls in a CMSR control family (such as Risk Assessment) the reference is written as "Risk Assessment policies and procedures". References about more specific policies, such as security control testing, are written as "policies and procedures regarding security control testing".

The required documentation includes, but is not limited to the following:

3.3.1 GLOBALLY APPLICABLE DOCUMENTATION

1) FISMA Evaluation with CMS Minimum Security Requirements (CMSR) using the CMS Integrated Security Suite (CISS)
2) Employee lists for Medicare, information systems, and information system security departments (lists shall include: name or identification (ID) number, job title, department, start date, and position effective date)
3) Human Resource (HR) policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
4) Evidence supporting resolution of prior year audit findings
5) Evidence supporting the ongoing employment of controls and control processes.
6) System generated reports of current security configuration settings
7) System generated reports (on request) for selected user populations and/or selected access capabilities.

3.3.1 DOCUMENTATION FOR GENERAL CONTROLS

3.3.1.1 SECURITY MANAGEMENT (SM)

SM-1: Establish a security management program.

1) Documentation supporting the entitywide security management program
2) Security policies and entitywide security plan

3) The entity's organization chart (for the Medicare, information systems, and information system security departments: include names and titles)
4) Security budget documentation
5) Job descriptions for all positions with an information systems security roll
6) Documentation detailing security responsibilities and rules of behavior for: security officials, business owners, and users at the entitywide, GSS, and application levels
7) Agency/entity policies and procedures for preparing security plans
8) System (GSS) and application security plans
9) Entity systems inventory, including identification of all system interfaces

SM-2: Periodically assess and validate risks.

1) Risk Assessment policies and procedures
2) The most recent IS RAs and vulnerability analyses
3) Criteria used for revising risk assessments
4) Certification and accreditation documentation

SM-3: Document and implement security control policies and procedures.

1) Policies and procedures at the entitywide level, GSS, and application level

SM-4: Implement effective security awareness and other security-related personnel policies.

1) Documentation supporting or evaluating the awareness program
2) Current, signed security awareness statements
3) Hiring, transfer, and termination policies and procedures
4) Policies and procedures regarding confidentiality and/or security agreements
5) Policies and procedures regarding vacation
6) Documentation showing compliance with policies
7) System-generated list of users
8) List of active employees obtained from personnel
9) List of recently terminated and transferred employees obtained from personnel
10) Job descriptions for security management personnel
11) Job descriptions for a selection of other personnel relevant to the audit
12) Security training policies, procedures and training program documentation

13) Training records

SM-5: Monitor the effectiveness of the security program.

1) Policies and procedures regarding security control testing
2) Privacy impact assessments, including the methodology, a sample of test plan, and test results.
3) Most recent annual evaluation for FISMA
4) Most recent annual evaluation for privacy reporting

SM-6: Effectively remediate information security weaknesses.

1) Recent POA&Ms
2) Recent FMFIA reports
3) Prior year audit reports

SM-7: Ensure that activities performed by external third parties are adequately secure.

1) Policies and procedures pertaining to external third parties for the entitywide, system, and application levels
2) List of external third parties
3) Security provisions of external third party contracts

3.3.1.1 ACCESS CONTROLS (AC)

AC-1: Adequately protect information system boundaries.

1) Network schematics
2) Interface agreements
3) Systems documentation

AC-2: Implement effective identification and authentication mechanisms.

1) Policies and procedures regarding authentication of user identities
2) Policies and procedures regarding accounts (user, system, generic, default)
3) Policies and procedures regarding generating and communicating authenticators to users
4) Policies and procedures regarding generating and communicating passwords to users
5) List of settings for security parameters
6) Security logs

7) Evidence of review of logs and follow up action taken
8) Policies and procedures regarding handling lost or compromised authenticators
9) Policies and procedures regarding controlling and auditing concurrent logons from different workstations
10) Policies and procedures regarding generating and communicating certificates to users
11) Policies and procedures regarding controlling the display of authentication information

AC-3: Implement effective authorization controls.

1) List of access request approvers
2) Security reports of access rules for directory names for sensitive or critical files
3) List of recent changes to security access, authorizations, and related logs
4) Evidence of review of logs and follow up action taken
5) Security software parameters
6) Policies and procedures regarding generic and default accounts
7) System-generated list of inactive logon ids
8) List of recently terminated employees
9) Policies and procedures regarding file system access
10) Policies and procedures regarding emergency and temporary access
11) List of emergency or temporary (fire-call) IDs
12) Activity log of emergency or temporary IDs
13) Evidence of review of emergency or temporary ID logs and follow up action taken
14) Procedures for minimizing processes and services
15) Documentation describing the function and purpose of processes and services, and evidence of management approval
16) Evidence of review of user templates and/or profiles
17) Results of the last review of system programmer access capabilities

AC-4: Adequately protect sensitive system resources.

1) Policies and procedures regarding access to sensitive / privileged accounts
2) Security software settings to identify types of activity logged
3) Evidence of review of logs and follow up action taken
4) Media protection policies and procedures

5) Policies and procedures regarding cryptography (e.g., cryptographic tools, key management, authentication to cryptographic modules)

AC-5: Implement an effective audit and monitoring capability.

1) Incident Response policies and procedures
2) Audit and Accountability policies and procedures
3) System and Information Integrity policies and procedures
4) Policies and procedures regarding gathering forensic information
5) Qualifications of response team members and training records
6) Design and justification for the intrusion detection system
7) Report showing security software settings for auditable events
8) Audit records/logs
9) Security violation reports
10) Evidence of review of logs and reports for questionable activities and follow up action taken
11) List of recent alerts and advisories

AC-6: Establish adequate physical security controls.

1) Any facility risk assessments performed by the entity or by independent entities
2) Physical and environmental protection policies and procedures
3) Policies and procedures regarding non-employees
4) Policies and procedures regarding removal and return of storage media to and from the library
5) Tape library logs for the most recent 3 months
6) Policies and procedures regarding maintenance and accountability for storage of documents and equipment
7) Layout of entity buildings and overview of operations in each building
8) Computer network and telecommunications diagrams (physical and logical)
9) Facilities' environmental system diagrams (for example, HVAC)
10) Physical security awareness training records
11) Physical security awareness training program content
12) Physical security control procedures
13) The most recent self assessments and compliance review report

14) Appointment and verification procedures for visitors, contractors, and maintenance personnel
15) List of employees and contractors with badged access and the justification for such access
16) Emergency procedures
17) Fire drill documentation
18) Visitor entry logs (sign in and sign out logs) for facilities and sensitive areas
19) Evidence of review of visitor entry logs and follow up action taken
20) Documentation of changes of entry codes

3.3.1.2 CONFIGURATION MANAGEMENT (CM)

CM-1: Develop and document CM policies, plans, and procedures.

1) Configuration Management policies and procedures
2) Configuration management plan and documentation
3) SDLC methodology
4) Security configuration settings

CM-2: Maintain current configuration identification information.

1) Inventory of all computer assets
2) List of all vendor supplied software that indicates how current the software is
3) If available, integrity statements from vendors for all third party software

CM-3: Properly authorize, test, approve, track and control all configuration changes.

1) Configuration Management policies and procedures
2) System documentation
3) List of all systems software changes made during the fiscal year
4) Completed configuration management and software change request forms
5) For software change requests: specifications and related documentation
6) Test plan standards
7) For software change requests: test plans; test documentation; test transactions and data; test results
8) Documentation of management review and user acceptance
9) Procedures for distributing new software

10) Policies and procedures regarding configuration and program change control

11) List of libraries in use and associated access control lists.

12) Policies and procedures regarding user installed software and software usage restrictions

CM-4: Routinely monitor the configuration.

1) Policies and procedures relating to configuration verification and audit
2) Configuration verification and audit documents
3) Initial Program Load (IPL) procedures
4) Log from last IPL
5) Results of CA_EXAMINE runs

CM-5: Update software on a timely basis to protect against known vulnerabilities.

1) Policies and procedures regarding configuration change control
2) Policies and procedures regarding flaw remediation
3) List of vendor recommended patches to those installed on the system
4) List of patches installed on the system
5) Policies and procedures regarding malicious code protection
6) Policies and procedures regarding IPv6

CM-6: Appropriately document and approve emergency changes to the configuration.

1) Emergency change procedures
2) Emergency change log
3) Evidence of review of logs and follow up action taken
4) List of all emergency changes made during the fiscal year

3.3.1.3 SEGREGATION OF DUTIES (SD)

SD-1: Segregate incompatible duties and establish related policies.

1) Policies and procedures regarding segregation of duties
2) Entity organization chart showing information security functions and assigned personnel
3) Relevant alternate or back up job assignments
4) Data center operating procedures

5) Job descriptions for user security administrators and for several positions in organizational units

SD-2: Control personnel activities through formal operating procedures, supervision, and review.

1) Manuals that guide personnel in performing their duties
2) Access authorizations
3) The most recent access authorization review
4) Assessments regarding the adequacy of duty segregation
5) List of all current access to systems software
6) List of all users with access to migrate programs to production
7) List of all system programmers
8) List of all application programmers
9) List of all computer operators
10) List of all users with the ability to change security settings (administrators)

3.3.1.4 CONTINGENCY PLANNING (CP)

CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources.

1) Policies, procedures, and methodology regarding categorizing systems and creating the critical operations list
2) Contingency plans and other documentation supporting the critical operations list
3) Current business impact analysis
4) Contingency Planning policies and procedures
5) Continuity of operations plan

CP-2: Take steps to prevent and minimize potential damage and interruption.

1) Policies and procedures regarding backing up and transporting files
2) 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
3) Inventory records of files maintained off-site
4) Off-site documentation
5) Recovery capability test plan

6) Recovery capability test results
7) Policies and procedures regarding environmental control testing
8) Results of recent environmental controls tests
9) Rules for employee behavior in server rooms and other designated areas
10) Environmental control training records and training course documentation
11) Emergency response procedures
12) Emergency response procedure test policies
13) Emergency response procedure test results
14) Policies and procedures regarding hardware maintenance and copies of contracts with maintenance providers
15) Policies and procedures regarding problem management
16) Policies and procedures regarding change management

CP-3: Develop and document a comprehensive contingency plan.

1) Contingency Planning policies and procedures
2) Contingency plans
3) The most recent risk assessment
4) Emergency and temporary access authorizations

CP-4: Periodically test the contingency plan and adjust it as appropriate.

1) Policies, procedures and methodology regarding contingency plan testing
2) Results of the most recent contingency plan test
3) Updated contingency plan

3.3.2 DOCUMENTATION FOR BUSINESS PROCESS APPLICATION LEVEL CONTROLS

3.3.2.1 APPLICATION LEVEL GENERAL CONTROLS (AS)

AS-1: Implement effective application security management.

1) Application security plans
2) List of sensitive transactions for the business process being audited
3) The most recent security risk assessment for each application under assessment.

4) Policies and procedures regarding reviewing access to the application
5) Policies and procedures at the entitywide level, GSS, and application level
6) Policies and procedures regarding security control testing
7) Application security control test plans
8) Recent FMFIA/A-123 and POA&M (or equivalent) reports
9) Policies and procedures pertaining to external parties for the application under assessment
10) External reports (SAS 70) or other documentation supporting the results of compliance monitoring.

AS-2: Implement effective application access controls.

1) Application, and related entitywide and GSS, security plans
2) Policies and procedures regarding identification and authentication of users
3) Policies and procedures regarding account management
4) List of users and assigned IDs
5) Documentation of multiple log-ons and associated monitoring procedures
6) Policies and procedures regarding access authorization and control
7) Evidence of the effectiveness of periodic review of access by owners
8) Policies and procedures regarding public access
9) Policies and procedures regarding digital signatures
10) System-generated list of inactive logon IDs
11) List of recently terminated employees
12) List of users with access to identified sensitive transactions for the business process under assessment
13) Monitoring procedures
14) Report showing application parameters for logging and other controls
15) Application logs
16) Security violation reports
17) Evidence of review of logs and security violation reports and follow up action taken
18) Reports of authorized segregation of duty conflicts and sensitive process access

AS-3: Implement effective application configuration management.

1) Policies and procedures regarding application configuration management

2) Application configuration and related entity and GSS level configuration management information

3) Policies and procedures regarding SDLC

4) Dates of and training materials from the most recent SDLC training class

5) Application documentation

6) Policies and procedures regarding configuration change management

7) Policies and procedures regarding developer configuration management

8) Log of abends

9) Procedures for new software distribution

10) Change request forms for recent software modifications

11) Application test plan standards

12) List of libraries (e.g., production, test)

13) Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)

14) List of all authorized change request approvers

15) List of all users with access to library management software

16) List of all users with access to the production libraries (production code, source code, extra program copies)

17) Documentation for recent software changes

18) System reports of users with access to key programs, code, transactions and tables

19) Policies and procedures regarding monitoring changes

20) Monitoring reports or change logs that are reviewed

21) Evidence of review of monitoring reports and/or change logs and follow up action taken

AS-4: Segregate application user access to conflicting transactions and activities and monitor segregation.

1) Policies and procedures regarding segregation of duties

2) System generated list of security administrators and users with access to the application

3) Access authorizations

4) The most recent access authorization review

5) List of segregation of duty conflicts

6) If conflicts exist, documentation of roles and users with conflicts

7) If conflicts exist, monitoring controls that mitigate the conflicts

AS-5: Implement effective application contingency planning.

1) Contingency Planning policies, procedures, and methodology
2) Business Impact Assessment
3) Application contingency plan and broader scoped related plans
4) Contingency plan test results
5) Contingency plan test report

3.3.2.1 BUSINESS PROCESS CONTROLS (BP)

BP-1: Transaction data input is complete, accurate, valid, and confidential.

1) Policies and procedures regarding application data strategy
2) Application policies and procedures regarding source document and input file collection and preparation
3) List of application reports used to determine whether the necessary inputs are accepted for processing
4) Application procedures for reviewer overrides or bypassing data validation and error routines
5) Application data entry error handling procedures.

BP-2: Transaction data processing is complete, accurate, valid, and confidential.

1) Application configuration and/or design documentation
2) Application procedures for reviewer overrides or bypassing data processing routines
3) Application management review procedures
4) Application design document
5) Application procedures for reconciliations
6) Application policies and procedures over user-defined processing

BP-3: Transaction data output is complete, accurate, valid, and confidential.

1) Application policies and procedures regarding data output, retention and handling
2) Application policies and procedures regarding information integrity and confidentiality
3) Application policies and procedures regarding media protection
4) Tape library logs for the most recent 3 months

5) List of key application output/reports in the area of audit scope

6) List of users with access to key application output/reports.

BP-4: Master data setup and maintenance is adequately controlled.

1) Application documentation

2) Application policies and procedures regarding system and information integrity

3) Application policies and procedures regarding information accuracy, completeness, validity, and authenticity

4) Application policies and procedures regarding error handling

5) Application master data change reports

6) Application policies and procedures regarding segregation of duties

3.3.2.2 INTERFACE CONTROLS (IN)

IN-1: Implement an effective interface strategy and design.

1) Application documentation

2) Application policies and procedures regarding information integrity

IN-2: Implement effective interface processing procedures.

1) Application documentation

2) Application policies and procedures regarding information integrity

3) Interconnection service agreements and memorandums of understanding.

4) List of users who are assigned responsibility for the interfaces

5) List of individuals responsible for providing security surrounding the interfaces and these individuals' access permissions

6) Application reports or other documents used to reconcile interface processing between applications

7) Application procedures for correcting any rejected transactions.

8) Application audit trails

3.3.2.3 DATA MANAGEMENT SYSTEM CONTROLS (DA)

DA-1: Implement an effective data management system strategy and design

1) Documentation of the design of the data management system(s) associated with the application

2) List of access paths to data and sensitive data management system administrative functions and associated controls
3) Database security requirements and settings
4) Security event logging settings
5) Evidence of review of logs and follow up action taken
6) Policies, procedures and controls relating to monitoring the audit logs
7) Policies, procedures and controls relating to detecting abnormal activity
8) Documentation of any specialized data management processes used to facilitate interoperability

3.4 INTERVIEWS REQUIRED

The individuals will to be interviewed during phases of the information system control portion of a CFO Act audit depends on the contractor's role in the Medicare system and the division of audit task labor between the DHHS OIG and the contract auditor. However, in total it will be consistent with FISCAM interviews, which is presented in this section.

Some individuals' availability for interviews is globally applicable as their participation is called for in numerous tasks during the audit. These individuals are listed first. Because, interviews can span multiple topics, the list of people needed for interviews is presented at the control category level.

Individuals who will be called upon include, but are not limited to:

3.4.1 GLOBALLY AVAILABLE PERSONNEL

1) Medicare compliance officer
2) Person responsible for the Corrective Action Plan (CAP)
3) Person responsible for IS RA
4) Person responsible for the SSP
5) Person in charge of training (entity wide security program)
6) Internal audit lead
7) HR contact
8) Mainframe systems administrator
9) Mainframe security administrator
10) 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)

3.4.1 GENERAL CONTROLS INTERVIEWS

3.4.1.1 SECURITY MANAGEMENT (SM)

1) Information security management (the overall security manager and subordinate security managers responsible for specific systems and applications)

2) Security management staff

3) The official who conducted the most recent agency/entity vulnerability assessment

4) Appropriate entity management – regarding the methodology, criteria, procedures and controls for: including systems in, or excluding systems from, the systems inventory; and the completeness, accuracy, and currency of the inventory

5) Data owners, system administrators, and system users – regarding training received and awareness of security related responsibilities

3.4.1.1 ACCESS CONTROLS (AC)

1) Network administrator

2) System administrator

3) Security managers

4) Incident response team members

5) Officials with system and communication responsibilities

6) Personnel with media responsibility

7) It management and security personnel (in consultation) - to identify control points; determine whether the access paths and related system documentation is up-to-date, properly approved by management, and consistent with risk assessments.

8) Appropriate users of the system – regarding aspects of various types of connectivity and authentication

9) Resource owners - regarding periodic reviews of access authorizations for continuing appropriateness

10) Technical management and systems staff - regarding access restrictions to sensitive system resources

11) Appropriate personnel – regarding media labeling

12) Appropriate officials - regarding the pickup, transport, and delivery of information system media (paper and electronic)

13) Appropriate officials – regarding authentication to a cryptographic module

14) Senior management and personnel responsible for summarizing violations and incidents – regarding the analysis, and communication of security violations and incidents

15) Entity officials - regarding how their physical security program is organized and whether a risk management approach is used

16) Appropriate officials – regarding identification of all significant threats to the physical well-being and determination of related risks

17) Appropriate officials – regarding established law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies

18) Appropriate officials – regarding protecting against emerging threats, such as CBR (chemical, biological, radiation) attacks, based on risk

3.4.1.2 CONFIGURATION MANAGEMENT (CM)

1) CM management and software development staff

2) Users

3) Data processing staff

4) Library control personnel.

5) Personnel responsible for appropriate tools and library control.

6) Appropriate staff - regarding configuration management training

7) Hardware and software managers - regarding the currency and completeness of CM policies, plans, procedures, and documentation

8) Users – regarding availability software change requests, test reports, and configuration items associated with the various baselines being managed.

9) Appropriate officials - regarding the criteria and methodology used for scanning, tools used, frequency, recent scanning results, and related corrective actions.

3.4.1.3 SEGREGATION OF DUTIES (SD)

1) Security managers
2) Selected systems support personnel
3) Selected user personnel
4) Selected supervisors and personnel
5) Selected management and information security personnel - regarding segregation of duties
6) Management - regarding compensating controls
7) Management personnel - regarding job descriptions
8) Personnel filling positions for selected job descriptions
9) Selected personnel - regarding provision of adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties
10) Management personnel - regarding responsibilities for restricting access by job positions in key operating and programming activities
11) Supervisors regarding review of user activity logs for incompatible actions

3.4.1.4 CONTINGENCY PLANNING (CP)

1) Information security program officials
2) Information technology officials
3) Security administration officials
4) Site managers
5) Security personnel
6) Appropriate support staff
7) Operational staff
8) Data center management and staff
9) Information security management
10) Data processing management
11) User management
12) Senior management

13) Program managers

14) Officials responsible for contingency plan related contracts, agreements, and logistics

15) Entity officials - regarding the existence of comprehensive procedures and mechanisms to fully restore the information security to its original state

3.4.2 BUSINESS PROCESS APPLICATION LEVEL CONTROLS INTERVIEWS

3.4.2.1 APPLICATION LEVEL GENERAL CONTROLS (AS)

1) Application owners

2) Security administrators

3) Information security program officials

4) Information technology officials

5) Security administration officials

6) Management responsible for security testing

7) Management responsible for Corrective Action Plans

8) Senior management - regarding contingency plan test results

9) Entity management - regarding policies and procedures to review access to the application

10) Application users - regarding awareness of application security policies

11) Appropriate management - regarding procedures used to monitor third party providers

12) Appropriate personnel - regarding segregation of application duties

13) Appropriate personnel - regarding key transactions that provide user access to change application functionality

14) Appropriate personnel - regarding key programs and tables for the application

15) Appropriate personnel - regarding system administration transactions

16) Appropriate management - regarding identification of incompatible activities and transactions

17) Application developers - regarding how the application segregates users from performing incompatible duties.

3.4.2.1 BUSINESS PROCESS CONTROLS (BP)

1) Application user management

2) Application users

3) Application data processing operations management

4) Application technical management - regarding data strategy

3.4.2.2 INTERFACE CONTROLS (IN)

1) Application user management

2) Application data processing operations management

3.4.2.3 DATA MANAGEMENT SYSTEM CONTROLS (DA)

1) None

3.5 SPACE AND EQUIPMENT REQUIREMENTS

Some of the requirements for space and equipment include the following:

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

4 SECTION 912 EVALUATION

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

The CMS-contracted auditor has agreed to perform procedures established by CMS and the DHHS OIG associated with the eight FISMA statutory areas which include:

1) Periodic IS RAs;

2) Policies and procedures based on IS RAs that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the systems development life cycle and complies with the NIST standards;

3) System Security Plans;

4) Security awareness training;

5) Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities;

6) Remedial activities, processes and reporting for deficiencies;

7) Incident detection, reporting and response; and

8) Continuity of operations for IT systems.

4.1 SITE SELECTION CRITERIA

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

4.1 AUDIT STEPS AND OBJECTIVES

4.1.1 RISK ASSESSMENTS

1) Determine if the current system configuration is documented, including links to other systems.

2) Determine if IS RAs 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.

4.1.1 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 IS RAs 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.

4.1.2 REVIEW OF SYSTEM SECURITY PLANS

1) Determine if a security plan is documented and approved.

2) Determine if the plan is kept current.

3) Determine if a security management structure has been established.

4) Determine if IS 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.

4.1.3 REVIEW OF SECURITY AWARENESS TRAINING

1) Determine if employees have received a copy of the Rules of Behavior (ROB).

2) Determine if employee training and professional development has been documented and formally monitored.

3) Determine if there is mandatory annual refresher training for security.

4) Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.

5) Determine if employees have received a copy of or have easy access to agency security procedures and policies.

6) Determine if security professionals have received specific training for their job responsibilities, and if the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.

4.1.4 REVIEW OF PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF IT SECURITY POLICIES

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

4.1.5 REVIEW OF REMEDIAL ACTIVITIES, PROCESSES, AND DEFICIENCY REPORTING

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

4.1.6 REVIEW OF INCIDENT DETECTION, REPORTING, AND RESPONSE

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

4.1.7 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 contingency plan is periodically tested.
12) Determine if the results are analyzed and the contingency plans are adjusted accordingly.
13) Determine if physical security controls exist to protect IT resources.

4.2 TESTING PROCEDURES

Refer to Appendix III for detailed testing procedures.

4.3 DOCUMENTATION

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

4.3.1 RISK ASSESSMENT REVIEW

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

4.3.1 POLICIES AND PROCEDURES

1) IT Security
2) Job descriptions for management

4.3.2 SYSTEM SECURITY PLAN

1) SSP
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

4.3.3 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)

4.3.4 REVIEW OF PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF IT SECURITY POLICIES AND PROCEDURES INCLUDING NETWORK ASSESSMENTS AND PENETRATION ACTIVITIES

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

4.3.5 REVIEW OF REMEDIAL ACTIVITIES, PROCESSED AND REPORTING FOR DEFICIENCIES

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

4.3.6 REVIEW OF INCIDENT DETECTION, REPORTING AND RESPONSE

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

4.3.7 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

4.4 INTERVIEWS REQUIRED

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

1) Medicare compliance officer
2) Person responsible for the CAP
3) Person responsible for IS RA
4) Person responsible for the SSP
5) Person in charge of training (entity wide security program)
6) Internal audit lead
7) HR contact
8) Mainframe systems administrator
9) Mainframe security administrator
10) LAN administrator
11) LAN security officer
12) Security software administrator
13) Systems programming manager
14) Person in charge of maintaining the System and Business Continuity Plan
15) Person in charge of the data center

16) Manager of physical security

17) Head of computer operations

18) Person in charge of change management

19) Application manager for the following systems:

    a) FISS

    b) MCS

    c) VMS

4.5 SPACE AND EQUIPMENT REQUIREMENTS

Some of the requirements for space and equipment include the following:

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.

5 SAS 70 AUDITS

SAS 70, is an internationally recognized auditing standard developed by the AICPA. A SAS 70 audit or service auditor's examination is widely recognized because it indicates that a service organization has been through an in-depth audit of IT control activities and related processes.

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

FISMA Note: Per OMB Memorandum M-08-21: SAS 70 audits may or may not meet the requirements of FISMA. … In determining whether SAS 70 reports provide sufficient evidence of contractor system FISMA compliance, it is the agency’s responsibility to ensure:

- The scope of the SAS 70 audit was sufficient, and fully addressed the specific contractor system requiring FISMA review.

- The audit encompassed all controls and requirements of law, OMB policy and NIST guidance.

5.1 SITE SELECTION CRITERIA

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

5.1 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:

- Security Management
- Access Controls
- Configuration Management
- Segregation of Duties
- Contingency Planning
- Application Level General Controls (also called Application Security)
- Business Process Controls
- Interface Controls
- Data Management System Controls.

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 significant computerized applications (such as claims processing), accounting systems, 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. Application level controls must ensure completeness, accuracy, and authorization.

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).

5.2 TESTING PROCEDURES

Please refer to Appendix IV for detailed testing procedures.

5.3 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., SSP)
2) Network diagrams
3) IS RAs and vulnerability analyses
4) Organizational charts that include names and titles for the Medicare, information systems, and information system security departments
5) Completed CMSRs using the CISS
6) IS RA 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 IS RA reports
10) Policies and procedures regarding conduct in the data center

11) Policies and procedures for back-up tape rotation and off-site storage

12) Policies and procedures for sanitation of media prior to disposal

13) Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms

14) Policies and procedures regarding visitors to both the general campus and to the sensitive areas

15) Layout of company buildings and overview of operations in each building

16) Employee lists for Medicare, information systems, and information system security departments (lists shall include: name or identification (ID) #, job title, department, start date, and position effective date)

17) Documentation of new hire/information system security training program

18) Vendor sign in and sign out logs for maintenance or repairs in sensitive areas

19) Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract

20) Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests

21) Policies and procedures regarding the testing of the plan

22) Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable

23) Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

24) Security policies, standards, and procedures for:

    a) Creation, modification, and deletion of user-IDs, functional groups, etc.

    b) Periodic review of access

    c) Dial-up access

    d) Use and monitoring of emergency or temporary access (Fire-call IDs)

    e) Password composition/mask

    f) Violation and security monitoring

    g) Archiving, deleting, or sharing data files

    h) Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)

25) List of all terminations during the current fiscal year

26) List of all transfers during the current fiscal year

27) List of all new hires during the current fiscal year

28) List of all Medicare application users

29) List of all users with dial up access

30) List of all users with the ability to change security settings (administrators)

31) Access to access requests and authorizations (for a sample of users)

32) List of access request approvers

33) Documentation supporting recertification of users

34) List of emergency or temporary (fire-call) IDs

35) Activity log of emergency or temporary IDs

36) Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties

37) System default password requirements

38) Use of generic, group or system IDs

39) Database security requirements and settings

40) Security violation logging and monitoring

41) Evidence of review of user templates and/or profiles

42) Evidence of automatic timeout on terminals

43) Database access lists

44) Evidence supporting resolution of prior year audit findings

45) Results of CA_EXAMINE runs

46) Policies and procedures for restricting access to systems software

47) A list of all system programmers

48) A list of all application programmers

49) A list of all computer operators

50) Results of the last review of system programmer access capabilities

51) A list of all vendor supplied software indicating the current version of the software

52) If available, integrity statements from vendors for all third party software

53) Policies and procedures for using and monitoring use of system utilities

54) Policies and procedures for identifying, selecting, installing and modifying systems software

55) Policies and procedures for disabling vender supplied defaults

56) Roles and responsibilities for system programmers

57) Policies and procedures for emergency software changes

58) A list of all systems software changes made during the fiscal year

59) A list of all emergency changes made during the fiscal year

60) A list of all current access to systems software

61) A list of all users with access to migrate programs to production

62) A sample of audit logs for system utilities and system programmer activity

63) Evidence of review of logs and follow up action taken

64) IPL procedures

65) Log from last IPL

66) 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

5.4 INTERVIEWS REQUIRED

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

1) Medicare compliance officer
2) Person responsible for the CAP
3) Person responsible for IS RA
4) Person responsible for the SSP
5) Person in charge of training (entity wide security program)
6) Internal audit lead
7) HR contact
8) Mainframe systems administrator
9) Mainframe security administrator
10) LAN administrator

11) LAN security officer

12) Security software administrator

13) Systems programming manager

14) Person in charge of maintaining the System and Business Continuity Plan

15) Person in charge of the data center

16) Manager of physical security

17) Head of computer operations

18) Person in charge of change management

19) Application manager for the following systems:

    a) FISS

    b) MCS

    c) VMS

5.5 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.

6 PENETRATION/EVA

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

6.1 EXECUTION OF THE AUDIT

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

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.

6.1 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 that their controls are also understood, but such sites are not likely to be audited every year.

6.2 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 shall 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 shall be conducted from either a CMS-contracted auditor lab or the client site. Identify the source Internet Protocol (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) **shall 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 file system 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.

6.3 DOCUMENTATION

Documentation and other items needed for Penetration/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 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.
4) System administrator/programmer access for systems to perform diagnostic review.
5) 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.

6.4 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

6.5 SPACE AND EQUIPMENT REQUIREMENTS

1) Workspace for each member of the audit team – usually one Senior Associate and one Associate
2) At least one telephone line, and network connectivity

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

(This Page Intentionally Blank)

APPENDIX I: CFO GENERAL CONTROLS TESTING PROCEDURES

General Controls are applicable to the entitywide and system levels. They are the policies, procedures, and other controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.

Control Activity	Control Techniques	Assessment Procedures	CMSR
Security Management (SM)			
SM-1: Establish a security management program.			

SM-1.1: The security management program is adequately documented, approved, and up-to-date.	SM-1.1.1: An agency/entitywide security management program has been developed, documented, and implemented that
	• covers all major facilities and operations,
	• has been approved by senior management and key affected parties, and
	• covers the key elements of a security management program:
	  • periodic risk assessments,
	  • adequate policies and procedures,
	  • appropriate subordinate information security plans,
	  • security awareness training,
	  • management testing and evaluation,
	  • a remedial action process,
	  • security-incident procedures, and
	  • continuity of operations.
		1) Review documentation supporting the agency/entitywide security management program and discuss with key information security management and staff.
		2) Determine whether the program
		• adequately covers the key elements of a security management program
		• is adequately documented, and
		• is properly approved.
		3) Determine whether all key elements of the program are implemented. Consider audit evidence obtained during the course of the audit.
			• AC-1, AT-1,
			• AU-1, CA-1,
			• CM-1, CP-1,
			• IA-1, IR-1,
			• MA-1, MP-1,
			• PE-1, PL-1,
			• PL-2, PL-3,
			• PL-6, PS-1,
			• RA-1, SA-1,
			• SA-2, SC-1,
			• SI-1

	SM-1.1.2: The agency/entitywide security management program is updated to reflect current conditions.	1) Based on a review of security management program documentation and interviews with key information security management and staff, determine whether the entity has adequate policies and procedures to identify significant changes in its IT environment that would necessitate an update to the program, and	• PL-3

		whether the program is periodically updated to reflect any changes.	
• SM-1.2: A security management structure has been established.	• SM-1.2.1: Senior management establishes a security management structure for the entitywide, system, and applications that has adequate independence, authority, expertise, and resources.	1) Review security policies and plans, the entity's organization chart, and budget documentation. Interview security management staff. Evaluate the security structure: independence, authority, expertise, and allocation of resources required to adequately protect the information systems.	• PS-CMS-2, • SA-2
	• SM-1.2.2: An information systems security manager has been appointed at an agency/entity level and at appropriate subordinate (i.e., system and application) levels and given appropriate authority.	1) Review pertinent organization charts and job descriptions. Interview the overall security manager and subordinate security managers responsible for specific systems and applications.	• PS-CMS-2
• SM-1.3: Information security responsibilities are clearly assigned.	• SM-1.3.1: The security program documentation clearly identifies owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined at the entitywide, system, and application levels for (1) information resource owners and users, (2) information technology management and staff, (3) senior management, and (4) security administrators.	1) Review security program documentation detailing security responsibilities and rules of behavior for security officials, resource owners, and users at the entitywide, system, and application levels.	• PL-1, PL-2
• SM-1.4: Subordinate security plans are documented, approved, and kept up-to-date.	• SM-1.4.1: System and application security plans have been documented and implemented that • cover all major facilities and operations, • have been approved by key affected parties, • cover appropriate topics (for federal agencies, those prescribed by OMB Circular A-130; see table 4).	1) Review agency/entity policies and procedures for preparing security plans. Review the system and application security plans encompassing key areas of audit interest and critical control points. Determine whether the plans adequately cover appropriate topics (for federal agencies, those prescribed by OMB Circular A-130) and are properly approved. When conducting the audit, determine whether the plans have been implemented and accurately reflect the conditions noted.	• PL-2
	• SM-1.4.2: The subordinate security plans are updated on a regular basis or whenever there are significant changes to the agency/entity policies, organization, IT systems, facilities,	1) Review relevant security plans and any related documentation indicating whether they have been reviewed and updated and are current.	• PL-3

	applications, weaknesses identified, or other conditions that may affect security.		
• SM-1.5: An inventory of systems is developed, documented, and kept up-to-date.	• SM-1.5.1: A complete, accurate, and up-to-date inventory exists for all major systems that includes the identification of all system interfaces.	1) Obtain the agency's/entity's systems inventory. Discuss with agency/entity management (1) the methodology and criteria for including or excluding systems from the inventory and (2) procedures and controls for ensuring the completeness, accuracy, and currency of the inventory. Determine whether systems tested during the audit are included in the inventory. Test the inventory for completeness, accuracy, and currency. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's process and controls for ensuring the accuracy of the inventory.	• CA-3, CM-8
• SM-2: Periodically assess and validate risks.			
• SM-2.1: Risk assessments and supporting activities are systematically conducted.	• SM-2.1.1: Appropriate risk assessment policies and procedures are documented and based on security categorizations.	1) Review risk assessment policies, procedures, and guidance.	• RA-1, RA-2
	• SM-2.1.2: Information systems are categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals.	1) Determine if security risk categorizations are documented and, for federal entities, if they comply with FISMA, NIST FIPS Pub 199 and SP 800-60.	• RA-2
	• SM-2.1.3: Risks are reassessed for the entitywide, system, and application levels on a periodic basis or whenever systems, applications, facilities, or other conditions change.	1) Obtain the most recent risk assessments encompassing key areas of audit interest and critical control points. Determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by sufficient testing. For federal systems, consider compliance with FISMA, OMB, and NIST requirements/guidance and whether the technology used is appropriately considered in the risk assessment and validations. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is	• CA-4, CA-6, • RA-3, RA-4

			generally limited to understanding management's risk assessment process (including related controls), reading the risk assessments for the key systems relevant to the audit objectives, and determining whether risks identified by the IS controls audit are properly considered in the risk assessments.	
	• SM-2.1.4: Risk assessments and validations, and related management approvals are documented and maintained on file. Such documentation includes security plans, risk assessments, security test and evaluation results, and appropriate management approvals.	1)	For a selection of risk assessments determine whether required management approvals are documented and maintained on file.	• CA-4, CA-6, • RA-3, RA-4
	• SM-2.1.5: Changes to systems, facilities, or other conditions and identified security vulnerabilities are analyzed to determine their impact on risk and the risk assessment is performed or revised as necessary based on OMB criteria.	1)	Review criteria used for revising risk assessments. For recent changes that meet the criteria, determine if the risk assessment was redone or updated.	• RA-4
	• SM-2.1.6: Federal systems are certified and accredited before being placed in operation and at least every 3 years, or more frequently if major system changes occur.	1)	For federal systems that are significant to the audit objectives, review certification and accreditation documentation and determine compliance with NIST SP 800-37. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding the certification and accreditation process (including related controls), reading the certifications and accreditations for the key systems relevant to the audit objectives, and determining whether the certification and accreditation documentation for the systems tested is consistent with the testing results.	• CA-4, CA-6
• SM-3: Document and implement security control policies and procedures.				
• SM-3.1: Security control policies and procedures are	• SM-3.1.1: Security control policies and procedures at all levels • are documented,	1)	Review security policies and procedures at the entitywide level, system level and application level. Compare the content of the policies and procedures to NIST guidance (e.g. SP 800-30,	• AC-1, AT-1, • AU-1, CA-1, • CM-1, CP-

documented, approved by management and implemented.	• appropriately consider risk, • address purpose, scope, roles, responsibilities, and compliance, • ensure that users can be held accountable for their actions, • appropriately consider general and application controls, • are approved by management, and • are periodically reviewed and updated.	SP 800-37,SP 800-100) and other applicable criteria (e.g. configuration standards).	1, • IA-1, IR-1, • MA-1, MP-1, • PE-1, PL-1, • PS-1, RA-1, • SA-1, SC-1, • SI-1
• SM-4: Implement effective security awareness and other security-related personnel policies.			
• SM-4.1: Owners, system administrators, and users are aware of security policies.	• SM-4.1.1: An ongoing security awareness program has been implemented that includes security briefings and training that is monitored for all employees with system access and security responsibilities. Coordinate with the assessment of the training program in SM-4.3.	1) Review documentation supporting or evaluating the awareness program. Observe a security briefing. 2) Interview data owners, system administrators, and system users. Determine what training they have received and if they are aware of their security-related responsibilities.	• AT-2, AT-3, • AT-4, PL-4, • PS-6, PS-7
	• SM-4.1.2: Security policies are distributed to all affected personnel, including system and application rules and expected user behaviors.	1) Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. If appropriate, call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.	• PL-4, PS-6
• SM-4.2: Hiring, transfer, termination, and performance policies address security.	• SM-4.2.1: For prospective employees, references are contacted and background checks performed. Individuals are screened before they are given authorization to access organizational information and information systems.	1) Review hiring policies. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.	• PS-3
	• SM-4.2.2: Periodic reinvestigations are performed as required by law, and implementing regulations [at least once every 5 years], consistent with the sensitivity of the position per criteria from the Office of Personnel Management (OPM).	1) Review applicable laws, regulations and reinvestigation policies (e.g. 5CFR 731.106(a); OPM/Agency policy, regulations and guidance; FIPS 201 & NIST SP 800-73, 800-76, 800-78; and, any criteria established for the risk designation of the assigned position.) For a	• PS-2, PS-3

		selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed as required.	
	• SM-4.2.3: Nondisclosure or security access agreements are required for employees and contractors assigned to work with confidential information.	1) Review policies on confidentiality or security agreements. For a selection of such users, determine whether confidentiality or security agreements are on file.	• PS-6
	• SM-4.2.4: When appropriate, regularly scheduled vacations exceeding several days are required, and the individual's work is temporarily reassigned.	1) Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed employee's work during vacations.	• PS-1
	• SM-4.2.5: A formal sanctions process is employed for personnel failing to comply with security policy and procedures.	1) Review the sanctions process. Determine how compliance with security policies is monitored and how sanctions were administered.	• PS-8
	• SM-4.2.6: Where appropriate, termination and transfer procedures include- exit interview procedures;- return of property, keys, identification cards, passes, etc.;- notification to security management of terminations and prompt revocation of IDs and passwords;- immediate escort of terminated employees out of the agency's facilities; and- identification of the period during which nondisclosure requirements remain in effect.	1) Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine whether IDs and passwords for terminated employees still exist.	• AC-2, PE-3, • PS-4, PS-5
• SM-4.3: Employees have adequate training and expertise.	• SM-4.3.1: Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	1) Review job descriptions for security management personnel and for a selection of other personnel. For a selection of employees, compare personnel records on education and experience with job descriptions.	• PS-1
	• SM-4.3.2: A security training program has been developed and includes first-time security awareness training entitywide for all new employees, contractors, and users before they are authorized to access the system, and periodic refresher training thereafter; technical training for personnel	1) Review training program documentation. See NIST SP 800-16 and 800-50 for guidance. Coordinate with the assessment of security awareness in SM-4.1.	• AT-2, AT-3

	with significant system roles and responsibilities before they are authorized access to the system; and periodic refresher training thereafter; and documented entitywide security training records that are monitored for all employees who have system access and security responsibilities.		
	• SM-4.3.3: Employee training and professional development are documented and monitored.	1) Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.	• AT-4
• SM-5: Monitor the effectiveness of the security program.			
• SM-5.1: The effectiveness of security controls are periodically assessed.	• SM-5.1.1: Appropriate monitoring and testing policies and procedures are documented.	1) Review testing policies and procedures. Determine if there is an overall testing strategy or plan.	• CA-2, CA-7, • RA-5, SA-11
	• SM-5.1.2: Management routinely conducts vulnerability assessments and promptly corrects identified control weaknesses.	1) Interview officials who conducted the most recent agency/entity vulnerability assessment. Review the methodology and tools used, test plans and results obtained, and corrective action taken. 2) Determine if testing is performed that complies with OMB and NIST certification and accreditation and other testing requirements. 3) If appropriate, perform independent testing with the approval of management. 4) Determine if identified control weaknesses are promptly corrected.	• CA-2, CA-5, • RA-5
	• SM-5.1.3: Management routinely conducts privacy impact assessments and promptly corrects identified control weaknesses.	1) Review privacy impact assessments, including the methodology, a sample of test plan, and related testing results.	• PL-5
	• SM-5.1.4: The frequency and scope of security control testing is commensurate with risk.	1) Determine if control testing is based on risk.	• CA-2, CA-4
	• SM-5.1.5: Performance measures and compliance metrics monitor the security processes and report on the state of compliance in a timely manner.	1) Review agency/entity performance measures and compare to OMB's performance measures and NIST guidance.	• AU-6, CA-2, • CA-7, CM-4, • IR-5, PE-6,

			• RA-5, SI-4, • SI-5
	• SM-5.1.6: An annual independent evaluation of the federal agency's information security program tests the effectiveness of the security policies, procedures, and practices.	1) Review the results of these annual evaluations for both FISMA and privacy reporting and any assessments of their adequacy and effectiveness.	• CA-4
	• SM-5.1.7: Federal agencies report on the results of the annual independent evaluations to appropriate oversight bodies. Under OMB guidance, the head of each agency must submit security and privacy reports to OMB, which consolidates the information for a report to Congress. The Comptroller General must also periodically evaluate and report to Congress on the adequacy and effectiveness of agency information security policies and practices.	1) Evaluate the reporting process and identify any significant discrepancies between reports at each level and whether the reports agree with independent audit evaluations. Note that OMB has annual requirements for FISMA and privacy reporting.	• CA-6
• SM-6: Effectively remediate information security weaknesses.			
• SM-6.1: Information security weaknesses are effectively remediated.	• SM-6.1.1: Management initiates prompt action to correct deficiencies. Action plans and milestones are documented.	1) Review recent POA&Ms, FMFIA reports and prior year audit reports and determine the status of corrective actions. The objective of this procedure in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's POAM process and related controls to ensure the accuracy of the information in the POA&Ms, determining whether IS control weaknesses identified by the IS controls audit are included in the POA&Ms, and, if not, determining the cause.	• CA-5
	• SM-6.1.2: Deficiencies are analyzed in relation to the entire agency/entity, and appropriate corrective actions are applied entitywide.	1) Evaluate the scope and appropriateness of corrective actions.	• CA-5
	• SM-6.1.3: Corrective actions are tested and are monitored after they have been implemented and monitored on a continuing basis.	1) Determine if implemented corrective actions have been tested and monitored periodically.	• CA-5

• SM-7: Ensure that activities performed by external third parties are adequately secure.			
• SM-7.1: External third party activities are secure, documented, and monitored.	• SM-7.1.1: Appropriate policies and procedures concerning activities of external third parties (for example, service bureaus, contractors, other service providers such as system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include provisions for • clearances, • background checks, • required expertise, • confidentiality agreements, • security roles and responsibilities, • connectivity agreements, • expectations, • remedies, • audit access/audit reporting, • termination procedures, and • security awareness training.	1) Review policies and procedures pertaining to external third parties for the entitywide, system, and application levels. 2) Identify use of external third parties and review activities including compliance with FISMA, and applicable policies and procedures. See NIST SP 800-35 for guidance on IT security services. 3) Determine how security risks are assessed and managed for systems operated by a third party. 4) Determine whether external third party services that relate to the technology are adequately controlled. 5) Coordinate assessment of security awareness training with SM-4.	• AC-20, AT-1, • MA-4, MA-5, • PS-3, PS-7, • SA-4, SA-9
	• SM-7.1.2: Security requirements are included in the information system acquisition contracts based on an assessment of risk.	1) Review security provisions of selected contracts and determine that requirements are implemented. See FAR requirements for acquisition plans (48 CFR 7.1, 7.103 (u).	• SA-4
• **Access Controls (AC)**			
• AC-1: Adequately protect information system boundaries.			
• AC-1.1: Appropriately control connectivity to system resources.	• AC-1.1.1: Connectivity, including access paths and control technologies between systems and to internal system resources, is documented, approved by appropriate entity management, and consistent with risk.	1) Review access paths in network schematics, interface agreements, systems documentation, and in consultation with IT management and security personnel identify control points; determine whether the access paths and related system documentation is up-to-date, properly approved by management, and consistent with risk assessments.	• CA-3

• AC-1.1.2: Networks are appropriately configured to adequately protect access paths within and between systems, using appropriate technological controls (e.g. routers, firewalls, etc.)	1) Interview the network administrator; determine how the flow of information is controlled and how access paths are protected. Identify key devices, configuration settings, and how they work together. (This step is a basis for the steps below). 2) Perform security testing by attempting to access and browse computer resources including critical files, security software, and the operating system. These tests may be performed as (1) an "outsider" with no information about the agency's computer systems, (2) an "outsider" with prior knowledge about the systems, and (3) an "insider" with and without specific information about the agency's computer systems and with access to the agency's facilities. Note: Due to the highly technical nature of such testing, it should be performed by an IT specialist. See FISCAM Appendix V for additional information. 3) 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 agency's computer resources using default/generic IDs with easily guessed passwords. See NIST SP 800-42 for more details. 4) When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, wireless, local area network, wide area network, and the Internet. See NIST SP 800-42 for more details.	• AC-4, AC-12, • SC-7, SC-10
• AC-1.1.3: The information system identifies and authenticates specific network devices before establishing a connection.	1) Determine whether authentication methods used are appropriate based on risk in accordance with FIPS Pub 200 and NIST SP 800-53.	• IA-3, • SC-CMS-6
• AC-1.1.4: Remote dial-up access is appropriately controlled and protected.	1) Interview network administrator and users; determine how remote dial-up access is controlled and protected (for example, monitor the source of calls and dial back mechanism);	• AC-17, • SC-CMS-6

	identify all dial-up lines through automatic dialer software routines and compare with known dial-up access; discuss discrepancies with management.	
• AC-1.1.5: Remote Internet access is appropriately controlled and protected.	1) Interview network administrator and users; determine how connectivity is controlled and protected. Determine if federal agency policies, procedures, and practices comply with NIST SP 800-63 guidance on remote electronic authentication. Also, refer to OMB Memorandum 04-04 E- Authentication Guidance for Federal Agencies.	• AC-17, • AC-19, • SC-7
• AC-1.1.6: Remote wireless access is appropriately controlled and protected.	1) Interview network administrator and users; determine how connectivity is controlled and protected. Refer to NIST SP 800-97 Establishing Wireless Robust Security Networks: A guide to IEEE.802.11i for additional security assessment guidance. Test and validate entity controls: (1) use a wireless sniffer to capture data (for example, service set IDs (SSID), (2) if an SSID is obtained, associate the SSID to the access point, (3) identify what network resources are available, (4) determine if a security protocol [FISCAM Footnote 76] is implemented, and (5) if a security protocol is used, employ a program to test the strength of the encryption algorithm. 2) Test and validate entity controls to identify rogue wireless access points. Test for rogue wireless access points. (See FISCAM Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this testing).	• AC-18
• AC-1.1.7: Connectivity is approved only when appropriate to perform assigned official duties. This includes portable and mobile devices, and personally-owned information systems. Appropriate safeguards are established to detect viruses, provide for	1) Interview network administrator and users; review justifications for a sample of connections. Determine if these systems use appropriate safeguards such as automatic updates for virus protection and up-to-date patch protection, etc.	• AC-19

	timely patch management, and other security measures are in place to validate appropriate access for users working remotely (e.g., home).		
• AC-1.2: Appropriately control network sessions.	• AC-1.2.1: The information system prevents further access to the system by initiating a session lock, after a specified period of inactivity that remains in effect until the user reestablishes access using identification and authentication procedures.	1) Observe whether the system automatically initiates a session lock during a period of inactivity, and how the user can directly initiate a session lock, and then unlock the session (See OMB M-06-16).	• AC-11, AC-12
	• AC-1.2.2: Where connectivity is not continual, network connection automatically disconnects at the end of a session.	1) Interview network administrator and users; observe whether the control is implemented.	• AC-12, SC-10
	• AC-1.2.3: Appropriate warning banners are displayed before logging onto a system • system use notification (for example, U. S. Government system, consent to monitoring, penalties for unauthorized use, privacy notices) • previous logon notification (for example, date and time of last logon and unsuccessful logons).	1) Interview network administrator and users; observe whether the control is fully implemented and complies with NIST guidance.	• AC-8, AC-9
• AC-2: Implement effective identification and authentication mechanisms.			
• AC-2.1: Users are appropriately identified and authenticated.	• AC-2.1.1: Identification and authentication is unique to each user (or processes acting on behalf of users), except in specially approved instances (for example, public Web sites or other publicly available information systems).	1) Review pertinent policies and procedures and NIST guidance pertaining to the authentication of user identities; interview users; review security software authentication parameters.	• IA-2, IA-3, • SC-14
	• AC-2.1.2: Account policies (including authentication policies and lockout policies) are appropriate given the risk, and enforced.	1) Review account policies and determine if they are based on risk and seem reasonable, based on interviews with system administrator and users. Determine how they are enforced, and test selected policies.	• AC-7, AC-10, • AC-14,AU-10, • IA-4, IA-5, • IA-6, SC-17, • SC-20,SC-21, • SC-22, SC-

			23
• AC-2.1.3: Effective procedures are implemented to determine compliance with authentication policies.	1)	Review adequacy of procedures for monitoring compliance with authentication policies; selectively test compliance with key policies.	• IA-4, IA-5
• AC-2.1.4: Selection of authentication methods (for example, passwords, tokens, biometrics, key cards, PKI certificates, or a combination therein) are appropriate, based on risk.	1)	Determine whether authentication methods used are appropriate, based on system risk levels determined by the entity using NIST FIPS 199. See NIST SP 800-53 authentication controls as specified for entity designated system risk levels.	• IA-2, IA-3
• AC-2.1.5: Authenticators are unique for specific individuals, not groups; • are adequately controlled by the assigned user and not subject to disclosure; and • cannot be easily guessed or duplicated. • Additional considerations for passwords are described below.	1)	Review pertinent entity policies and procedures; assess procedures for generating and communicating authenticators to users; interview users; review related security software parameters. Observe users using authenticators; attempt to logon without a valid authenticator. Assess compliance with NIST guidance on authenticator selection, content, and usage.	• IA-2, IA-4, • IA-5, IA-6
• AC-2.1.6: Password-based authenticators • are not displayed when entered; • are changed periodically (e.g., every 30 to 90 days); • contain alphanumeric and special characters; • are sufficiently long (e.g., at least 8 characters in length); • have an appropriate minimum life (automatically expire); • are prohibited from reuse for a specified period of time (e.g., at least 6 generations); and • are not the same as the user ID.	1)	Review pertinent entity policies and procedures; assess procedures for generating and communicating passwords to users; interview users; review security software password parameters. Observe users keying in passwords; attempt to logon without a valid password; make repeated attempts to guess passwords. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing). Assess entity compliance with NIST SP 800-63, which provides guidance on password selection and content.	• IA-5
• AC-2.1.7: Attempts to log on with invalid passwords are limited (e.g., 3–7 attempts).	1)	Examine security parameters for failed log-on attempts; review security logs to determine whether attempts to gain access are logged and reviewed by entity security personnel; if appropriate, repeatedly attempt to logon using	• AC-7

	invalid passwords.	
• AC-2.1.8: Use of easily guessed passwords (such as names or words) are prohibited.	1) As appropriate, review a system-generated list of current passwords; search password file using audit software to identify use of easily guessed passwords. Review management's controls to prevent or detect easily guessed passwords.	• IA-5
• AC-2.1.9: Generic user IDs and passwords are not used.	1) Interview users and security managers; review a list of IDs and passwords to identify generic IDs and passwords in use.	• IA-2
• AC-2.1.10: Vendor-supplied default passwords are replaced during installation.	1) Attempt to log on using common vendor-supplied passwords; search password file using audit software. (See FISCAM Section 2.2.2 "Appropriateness of Control Testing" for discussion of performance issues relating to this type of testing).	• AC-2
• AC-2.1.11: Passwords embedded in programs are prohibited. (Note: An embedded password is a password that is included into the source code of a program. Applications often need to communication with other applications and systems and this requires an "authentication" process which is sometimes accomplished through the use of embedded passwords).	1) Discuss with entity security management how it obtains reasonable assurance that there are no embedded passwords used. If used, determine whether procedures have been established to monitor their use. Review selected programs for embedded passwords.	• IA-3, SA-3
• AC-2.1.12: Use of and access to authenticators is controlled (e.g., their use is not shared with other users).	1) Review procedures to ensure that accounts are not shared. Select accounts to determine compliance with procedures.	• IA-5
• AC-2.1.13: Effective procedures are implemented to handle lost, compromised, or damaged authenticators (e.g., tokens, PKI certificates, biometrics, passwords, and key cards).	1) Identify procedures for handling lost or compromised authenticators; interview users and selectively test compliance with procedures.	• IA-5
• AC-2.1.14: Concurrent sessions are appropriately controlled.	1) Review procedures for controlling and auditing concurrent logons from different workstations.	• AC-10
• AC-2.1.15: Where appropriate, digital signatures, PKI, and electronic signatures are effectively implemented.	1) Determine how nonrepudiation is assured and if PKI and electronic/digital signatures are	• SC-17

		effectively implemented.	
	• AC-2.1.16: PKI-based authentication • validates certificates by constructing a certification path to an accepted trust anchor; • establishes user control of the corresponding private key; and • maps the authenticated identity to the user account.	1) Review pertinent entity policies and procedures; assess procedures for generating and communicating certificates to users; interview users; review security software certificate parameters; obtain the help of experts if needed.	• SC-17
	• AC-2.1.17: Authentication information is obscured (e.g., password is not displayed).	1) Review procedures for controlling the display of authentication information.	• IA-6
	• AC-2.1.18: Appropriate session-level controls are implemented (e.g., name/address resolution service, session authenticity)	1) Assess the adequacy of session-level controls to include name/address resolution service, session authenticity, protection of session level information held in temporary storage, and controls to ensure that one session ends before the next session begins (prevent overlapping sessions).	• SC-20,SC-21, • SC-22, SC-23
• AC-3: Implement effective authorization controls.			
• AC-3.1: User accounts are appropriately controlled.	• AC-3.1.1: Resource owners have identified authorized users and the access they are authorized to have.	1) These audit procedures should be coordinated with section 3.4 (segregation of duties) to ensure that users do not have access to incompatible functions. Review written policies and procedures; for a selection of users (both application and information security personnel), review access authorization documentation and applicable rights and privileges in the information system.	• AC-2
	• AC-3.1.2: Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs. (Standard naming	1) Determine directory names for sensitive or critical files and obtain security reports of related access rules. Using these reports, determine who has access to sensitive files and whether the access matches the level and type of access authorized. Determine whether standard naming conventions are established and used effectively.	• AC-2, AC-3

conventions are essential to ensure effective configuration management identification and control of production files and programs vs. test files and programs).		
• AC-3.1.3: Security managers review access authorizations and discuss any questionable authorizations with resource owners.	1) Interview security managers and review documentation provided to them to determine whether they review access authorizations to include follow-ups with resource owners on questionable authorizations.	• AC-2, AC-3, • AC-13
• AC-3.1.4: All changes to security access authorizations are automatically logged and periodically reviewed by management independent of the security function; unusual activity is investigated.	1) Review a selection of recent changes to security access authorizations and related logs for evidence of management review and unusual activity; determine if unusual activity is being/has been investigated.	• AC-13, AU-2, • AU-6
• AC-3.1.5: Resource owners periodically review access authorizations for continuing appropriateness.	1) Interview owners and review supporting documentation; determine whether they review access authorizations; determine whether inappropriate access rights are removed in a timely manner.	• AC-2, AC-3, • AC-13
• AC-3.1.6: Access is limited to individuals with a valid business purpose (least privilege).	1) Identify who has access to user accounts and sensitive system resources and the business purpose for this access.	• AC-6
• AC-3.1.7: Unnecessary accounts (default, guest accounts) are removed, disabled, or otherwise secured.	1) Verify that unnecessary accounts are removed, disabled, or secured.	• AC-2
• AC-3.1.8: Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	1) Review security software parameters; review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.	• AC-2, IA-4
• AC-3.1.9: Access to shared file systems are restricted to the extent possible (for example, only to particular hosts, and only for the level of access required).	1) Determine how access to shared file systems is restricted and verify that it works effectively.	• CM-7
• AC-3.1.10: Emergency or temporary access is appropriately controlled, including	1) Review pertinent policies and procedures; compare a selection of both expired and active	• AC-2

	• documented and maintained, • approved by appropriate managers, • securely communicated to the security function, • automatically terminated after a predetermined period, and • all activity is logged.	temporary and emergency authorizations (obtained from authorizing parties) with a system-generated list of authorized users. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed. Review procedures for monitoring the use of emergency/temporary IDs (including firecall IDs) to ensure that access was used properly to correct a problem.	
• AC-3.2: Processes and services are adequately controlled.	• AC-3.2.1: Available processes and services are minimized, such as through • installing only required processes and services based on least functionality, • restricting the number of individuals with access to such services based on least privilege, • monitoring the use of such services, and • maintaining current service versions. • Note; Installed processes and services should be consistent with approved system baseline.	1) Review procedures for minimizing processes and services; interview system administrator; identify what services are installed and determine if they are required; determine who has access to these services and if they need them; determine how access to these services is monitored; and determine if the service versions are kept current. If appropriate, scan for poorly configured, unnecessary, and dangerous processes and services.	• AC-6, CM-6, • CM-7, SC-6, • SC-14
	• AC-3.2.2: The function and purpose of processes and services are documented and approved by management.	1) Obtain documentation describing the function and purpose of processes and services, and evidence of management approval.	• CM-7
	• AC-3.2.3: Information available to potential unauthorized users is appropriately restricted.	1) Determine if information about available processes and services is appropriately restricted.	• AC-3, AC-14, • SC-14
	• AC-3.2.4: The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).	1) Determine if remote activation of collaborative computing services have been physically disconnected.	• SC-15
	• AC-3.2.5: For publicly available systems, the information system controls protect the integrity and availability of the information and applications.	1) Identify controls used to protect the integrity and availability of the information and applications on such systems and test controls to ensure their effectiveness.	• SC-14

• AC-4: Adequately protect sensitive system resources.			
• AC-4.1: Access to sensitive system resources is restricted and monitored.	• AC-4.1.1: Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose.	1) Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions. 2) Identify and test who has access to sensitive/privileged accounts and determine the reason for that access.	• AC-2, IA-4, • IA-7, SC-9, • SC-11, SC-12, • SC-16
	• AC-4.1.2: Use of sensitive/privileged accounts is adequately monitored.	1) Determine if the use of sensitive and privileged accounts is monitored and evaluate the effectiveness of monitoring procedures.	• AU-2, AU-6
	• AC-4.1.3: Logical access to utilities and tools is adequately controlled (for example, remote maintenance).	1) Determine the last time the access capabilities of system programmers were reviewed. 2) Review security software settings to identify types of activity logged. 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 application programmers and determine whether they are authorized access.	• AC-3, AC-6, • MA-3, MA-4
	• AC-4.1.4: Files relied upon by operating systems are appropriately controlled.	1) Determine if access to files relied upon by operating systems is adequately controlled.	• AC-3, AC-6, • CM-5, MP-2
	• AC-4.1.5: Passwords/authentication services and directories are appropriately controlled and encrypted when appropriate.	1) Determine if password files and authentication services are adequately protected from unauthorized access. Determine if password files are encrypted.	• AC-3
	• AC-4.1.6: Mobile code is appropriately controlled.	1) Interview system administrator and determine if mobile code is adequately controlled.	• SC-18
	• AC-4.1.7: Where appropriate, access is restricted based on time and/or location.	1) Determine if access is appropriately restricted based on time and/or location.	• AC-1, AC-2
	• AC-4.1.8: The information system partitions or separates user functionality (including user interface services) from information system management functionality.	1) Interview officials and review related system documentation. Coordinate with vulnerability analysis.	• SC-2, SC-4

	• AC-4.1.9: The information system isolates security functions from non-security functions.	1) Interview officials and review related system documentation. Coordinate with vulnerability analysis.	• SC-3
	• AC-4.1.10: The information system establishes a trusted communications path between the user and the security functionality of the system.	1) Interview officials with system and communication responsibilities and examine appropriate records such as developer design documents.	• SC-11
• AC-4.2: Adequate media controls have been implemented.	• AC-4.2.1: Only authorized users have access to printed and digital media removed from the information system.	1) Interview personnel and review procedures. Observe entity practices and review selected access logs.	• MP-2, MP-3
	• AC-4.2.2: The information system automatically identifies how information is to be used • output is marked using standard naming conventions, and • internal data in storage, process and transmission is labeled.	1) Interview appropriate personnel. For output, identify standard naming conventions and examine the system configuration. For internal data, examine the labeling mechanism and internal data for accurate labels. Test output and internal data for appropriate results.	• AC-15, AC-16
	• AC-4.2.3: The organization controls the pickup, transport, and delivery of information system media (paper and electronic) to authorized personnel.	1) Interview officials and review appropriate policy and procedures. Observe selected media transport practices and receipts.	• MP-5
	• AC-4.2.4: Systems media is securely stored according to its sensitivity.	1) Determine if media storage practices are adequate and comply with applicable requirements (for federal agencies, FIPS 199 security categories).	• MP-4
	• AC-4.2.5: Security parameters are clearly associated with information exchanged between information systems.	1) Determine if security parameters are clearly associated with information exchanged.	• SC-16
	• AC-4.2.6: Approved equipment, techniques, and procedures are implemented to clear sensitive data from digital media before its disposal or release for reuse outside of the organization.	1) Review written procedures; interview personnel responsible for clearing data from digital media. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and disposal of software. For selected items still in the agency's possession, test to determine whether they have been appropriately sanitized.	• MP-6
• AC-4.3:	• AC-4.3.1: Cryptographic tools have been	1) Determine if cryptographic tools are properly	• SC-8, SC-9,

Cryptographic controls are effectively used.	implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	implemented. (See NIST standards for federal agencies) To evaluate the use of cryptographic tools, the auditor should obtain the assistance of a specialist.	• SI-7
	• AC-4.3.2: Encryption procedures are implemented in data communications where appropriate based on risk.	1) Capture passwords transmitted over the network and determine if they are encrypted; for federal system, determine if cryptographic authentication complies with FIPS 140-2. To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.	• AC-17,AC-18, • MA-4, SC-9, • SC-13, • SC-CMS-3, • SC-CMS-4
	• AC-4.3.3: For authentication to a cryptographic module, the information system employs appropriate authentication methods.	1) Interview appropriate officials and review supporting documentation. For federal agencies, compare the authentication process to FIPS 140-2 requirements.	• IA-7, SC-13
	• AC-4.3.4: The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.	1) Compare policy and practices to appropriate guidance, such as NIST guidance in SP 800-56 and SP 800-57 for cryptographic key establishment and management, respectively.	• SC-12

- AC-5: Implement an effective audit and monitoring capability.

• AC-5.1: An effective incident response program is documented and approved.	• AC-5.1.1: An effective incident-response program has been implemented and include • documented policies, procedures, and plans; • documented testing of the incident response plan and follow-up on findings; • a means of prompt centralized reporting; • active monitoring of alerts/advisories; • response team members with the necessary knowledge, skills, and abilities; • training on roles and responsibilities and periodic refresher training; • links to other relevant groups; • protection against denial-of-service attacks (see http://icat.nist.gov); • appropriate incident-response assistance; and • consideration of computer forensics.	1) Interview security manager, response team members, and system users; review documentation supporting incident handling activities; compare practices to policies, procedures, and related guidance such as NIST SP 800-61 that provides guidance on incident-handling and reporting. 2) Determine qualifications of response team members; review training records; identify training in incident response roles and responsibilities. 3) Identify the extent to which computer forensics is used and compare to applicable guidelines and industry best practices.	• AT-5, IR-1, • IR-2, IR-3, • IR-4, IR-5, • IR-6, IR-7, • SC-5
• AC-5.2: Incidents are effectively identified and logged.	• AC-5.2.1: An effective intrusion detection system has been implemented, including appropriate placement of intrusion-detection sensors and incident thresholds.	1) Obtain the design and justification for the intrusion detection system; determine if the placement of sensors and incident thresholds is appropriate based on cost and risk.	• SI-4
	• AC-5.2.2: An effective process has been established based on a risk assessment, to identify auditable events that will be logged.	1) Interview the security manager to determine the process for determining what actions are logged. Determine if security event correlation tools are used to identify anomalous network activity.	• AU-2
	• AC-5.2.3: All auditable events, including access to and modifications of sensitive or critical system resources, are logged.	1) Review security software settings to identify types of activity logged; compare to NIST guidance on auditable events.	• AU-2
	• AC-5.2.4: Audit records contain appropriate information for effective review including sufficient information to establish what events occurred, when the events occurred (for example, time stamps), the source of the	1) Determine if audit records/logs are reviewed and whether they contain appropriate information; see NIST SP 800-92 for guidance.	• AU-3, AU-8

	events, and the outcome of the events.		
	• AC-5.2.5: Audit record storage capacity is adequate and configured to prevent such capacity from being exceeded. In the event of an audit failure or audit storage capacity being reached, the information system alerts officials and appropriate action is taken.	1) Determine the retention period for audit records and logs and whether it complies with applicable guidance. Determine if audit capacity is sufficient and what happens should it be exceeded.	• AU-4, AU-5, • AU-11
	• AC-5.2.6: Audit records and tools are protected from unauthorized access, modification, and deletion. Audit records are effectively reviewed for unusual or suspicious activity or violations.	1) Determine how access to audit records/logs is controlled; review logs for suspicious activity and evidence of entity follow-up and appropriate corrective action.	• AU-6, AU-9
	• AC-5.2.7: Audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	1) Determine if audit record retention (for example, logs etc.) meet legal requirements and entity policy for computer forensics. See General Records Schedule 20 and 24 for guidance on requirements for record retention. hyperlink, http://archives.gov/recordsmgmt/ardor/grs20.html and hyperlink, http://archives.gov/recordsmgmt/ardor/grs24.html.	• AU-11
• AC-5.3: Incidents are properly analyzed and appropriate actions taken.	• AC-5.3.1: Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported and investigated.	1) Review pertinent policies and procedures; review security violation reports; examine documentation showing reviews of questionable activities.	• AU-6
	• AC-5.3.2: Security managers investigate security violations and suspicious activities and report results to appropriate supervisory and management personnel.	1) Test a selection of security violations to verify that follow-up investigations were performed and reported to appropriate supervisory and management personnel.	• AU-6, PE-6
	• AC-5.3.3: Appropriate disciplinary actions are taken.	1) For the sample in AC-5.3.2, determine what action was taken against the perpetrator.	• PS-8
	• AC-5.3.4: Violations and incidents are analyzed, summarized, and reported to senior management and appropriate government authorities.	1) Interview senior management and personnel responsible for summarizing violations; review any supporting documentation. Determine if automated tools are used to analyze network activity and whether it complies with security policy.	• AU-6, AU-7
	• AC-5.3.5: Alerts and advisories are issued to	1) Identify recent alerts and advisories and	• SI-5

	personnel when appropriate.	determine if they are up-to-date; interview entity personnel to determine what actions were taken.	
	• AC-5.3.6: Incident and threat information is shared with owners of connected systems.	1) Determine if incident and threat data are shared with owners of connected systems; follow up with owners of connected systems to see if they received this information in a timely manner.	• IR-7, SI-5
	• AC-5.3.7: Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate.	1) Review policies and procedures and interview appropriate personnel; review any supporting documentation.	• IR-4
	• AC-5.3.8: Critical system resources are periodically reviewed for integrity.	1) Determine how frequently alterations to critical system files are monitored (for example, integrity checkers, etc.).	• AC-13, IR-5, • SC-5, SI-4, • SI-6
	• AC-5.3.9: Appropriate processes are applied to gather forensic evidence in support of investigations.	1) Review entity processes to gather forensic information and determine whether they are adequate. 2) Discuss with appropriate entity management.	• IR-4
• AC-6: Establish adequate physical security controls.			
• AC-6.1: Establish an effective physical security management program based on risk.	• AC-6.1.1: Use a risk management approach to identify the level of physical security needed for the facility and implement measures commensurate with the risks of physical damage or access.	1) Coordinate with sections SM-2 (assess and validate risks), SM-3 (policies and procedures), SD-1 (segregation of duties), and CP-2 (environmental controls). 2) Interview entity officials to discuss how their physical security program is organized and whether they use a risk management approach. Obtain and review any facility risk assessments performed by the entity or by independent entities.	• PE-1
	• AC-6.1.2: Facilities and areas housing sensitive and critical resources have been identified. The following generally constitute sensitive areas: computer rooms, tape libraries, telecommunication closets, mechanical/ electrical rooms, cooling facilities and data transmission and power lines.	1) Review diagram of physical layout of the computer network, telecommunications, and cooling system facilities (for example, HVAC); Inspect these areas for physical access control weaknesses.	• PE-3, PE-18

• AC-6.1.3: All significant threats to the physical well-being of these resources have been identified and related risks determined.	1) Interview entity officials. Review risk analysis to ensure that it includes physical threats to employees and assets. Review any recent audit reports or other evaluations of the facility's physical security.	• RA-3
• AC-6.1.4: Establish law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies, provide procedures for the timely receipt and dissemination of threat information, and implement a standardized security/threat classifications and descriptions (for example, alert levels).	1) Check if the organization has established law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies. Review how the organization receives and disseminates security alerts. Identify governmental agencies involved in the flow of security information and interview appropriate officials. Review procedures and nomenclature for threat information.	• PE-1
• AC-6.1.5: Conduct annual employee physical security awareness training. Coordinate this step with SM-4.	1) Review information (for example, individual training records, training program content) on security awareness training and its frequency.	• AT-1, AT-2
• AC-6.1.6: Security control procedures (for example, trusted vendors/suppliers, background checks, etc.) are established for non-employees (contractors, custodial personnel).	1) Review security control procedures for scope and adequacy.	• PS-3, PS-6, • PS-7
• AC-6.1.7: Periodic monitoring and independent evaluations of the physical security program are conducted. Physical security incidents are effectively monitored and appropriate countermeasures are implemented. .	1) Check if the agency evaluates its physical security program and controls. Obtain and review the agency's most recent self assessments and compliance review report. Determine if security incidents are recorded, effectively analyzed, and result in appropriate countermeasures. 2) Coordinate with SM-5: Monitor the effectiveness of the security program, and AC-5: Implement an effective audit and monitoring capability.	• CA-2, PE-6
• AC-6.1.8: When possible, do not co-locate high risk operations with non-essential support organizations (for example, cafeteria, day care, banks, news media). If not possible, place appropriate security between such	1) Identify co-located operations and their respective risk levels. Determine if the agency co-locates high risk operations with support operations and assess the security impact.	• PE-3, PE-18

	support organizations and critical facilities.		
	• AC-6.1.9: Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	1) Review appointment and verification procedures for visitors, contractors, and maintenance personnel. Compare actual practices to procedures.	• PE-2, PE-3
• AC-6.2: Establish adequate perimeter security based on risk.	• AC-6.2.1: Control/restrict vehicle and pedestrian traffic around the facility based on the facility's risk level. Specific measures include fences, gates, locks, guard posts, perimeter patrols and inspections.	1) Determine if vehicle and pedestrian traffic around the facility is adequately controlled for the risk level. Inspect the perimeter for physical security and access control weaknesses. Assess the effectiveness of perimeter guard procedures and practices for controlling access to facility grounds.	• PE-3
	• AC-6.2.2: Control employee and visitor parking. For example, restrict access to facility parking and parking adjacent to the facility (including leases), use ID systems and procedures for authorized parking (for example, placard, decal, card key), have signs and arrangements for towing of unauthorized vehicles and adequate lighting for parking areas.	1) Observe parking area and related controls. 2) Check if identification systems and procedures for authorized parking are in place. Determine what is done about unauthorized vehicles (e.g. towing).	• PE-2, PE-3, • PE-7
	• AC-6.2.3: Monitor the perimeter with closed circuit television (CCTV) including cameras with time lapse video recording and warning signs advising of 24 hour video surveillance.	1) Inspect the facility surveillance camera system to assess its capacity and ability to assist in protecting the facility's perimeter.	• PE-6
	• AC-6.2.4: Lighting is adequate for effective surveillance and evacuation operations. Emergency power backup exists for lighting (as well as for alarm and monitoring systems).	1) Observe perimeter and exterior building lighting to determine its adequacy. Also, determine if emergency power is available for security systems. Request test results.	• PE-6, PE-11, • PE-12
	• AC-6.2.5: Extend perimeter barriers (for example, concrete, steel) and parking barriers, as needed, to prevent unauthorized access and reduce exposure to explosions.	1) Determine if perimeter barriers are used and extended if appropriate.	• PE-3, PE-18
• AC-6.3: Establish adequate security at entrances and	• AC-6.3.1: All employee access is authorized and credentials (for example, badges, identification cards, smart cards) are issued to allow access.	1) Observe and document all access control devices used to secure the facility.	• PE-2, PE-3
	• AC-6.3.2: Access is limited to those	1) Observe entries to and exits from facilities	• PE-2, PE-3

	exits based on risk.	individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	during and after normal business hours. Obtain a list of employees and contractors with badged access and check the justification for such access. Check whether terminated employees/contractors have turned in their badge.	
		• AC-6.3.3: Management conducts regular reviews of individuals with physical access to sensitive facilities to ensure such access is appropriate.	1) Review procedures used by management to ensure that individuals accessing sensitive facilities are adequately restricted. 2) Evaluate support for physical access authorizations and determine appropriateness.	• PE-2
		• AC-6.3.4: Intrusion detection systems with central monitoring capability are used to control access outside of normal working hours (for example, nights and weekends).	1) Determine if an intrusion detection system is used and test its use for appropriate exterior and interior apertures.	• PE-6
		• AC-6.3.5: Visitor access logs are maintained and reviewed.	1) Compare entries in the log to a list of personnel authorized access.	• PE-8
		• AC-6.3.6: X-ray and magnetometer equipment is used to screen people, possessions, and packages.	1) Observe how this equipment is used and test its effectiveness.	• PE-3
		• AC-6.3.7: The entity controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.	1) Review procedures and interview officials. Attempt to enter and exit the facility with information systems items at various entry points and times.	• PE-16
		• AC-6.3.8: Entry and exit points are monitored by using CCTV capability. Also, high security locks and alarm systems are required for all doors that are not guarded.	1) Observe use of these devices and test as appropriate. Inspect the building(s) for physical access control weaknesses.	• PE-6
		• AC-6.3.9: Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter the facility after fire drills, etc.	1) Review written emergency procedures. 2) Examine documentation supporting prior fire drills. Observe a fire drill.	• PE-3
•	AC-6.4: Establish adequate interior security	• AC-6.4.1: An ID badge should generally be displayed at all times. [All individuals must display an ID at all times.]	1) Observe use of employee and visitor IDs. See what happens if you do not display your own ID.	• PE-1
		• AC-6.4.2: Visitors such as vendors,	1) Review visitor entry logs. Observe entries to	• PE-7, PE-8

based on risk.	contractors, and service personnel who need access to sensitive areas are prescreened, formally signed in, badged and escorted.	and exits from sensitive areas during and after normal business hours. Interview guards at facility entry.	
	• AC-6.4.3: Sensitive information technology and infrastructure resources are adequately secured (for example, using keys, alarm systems, security software and other access control devices), including • the badging system, • computer room, master consoles, and tape libraries, • display and output devices, • data transmission lines, • power equipment and power cabling, • mobile or portable systems, and • utility and mechanical areas (HVAC, elevator, water).	1) Interview officials. Walk through facilities and observe potential vulnerabilities and security controls [measures] used to protect sensitive information technology resources. 2) Observe entries to and exits from sensitive areas during and after normal business hours. Review security software features and settings. Evaluate the badging system: who has access to the badging system and how it is protected; how is physical control is maintained over unissued and visitor badges. Test the controls.	• PE-3, PE-4, • PE-5, PE-9, • PE-14, PE-15
	• AC-6.4.4: Management conducts regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate.	1) Review procedures used by management to ensure that individuals accessing sensitive areas are adequately restricted. 2) Determine if there is a periodic (e.g. annual) auditing and reconciliation of ID cards. Evaluate support for physical access authorizations and determine appropriateness.	• PE-2
	• AC-6.4.5: As appropriate, physical access logs to sensitive areas are maintained and routinely reviewed.	1) Compare entries in the logs to a list of personnel authorized access.	• PE-6
	• AC-6.4.6: Unissued keys, badges, or other entry devices are secured. Issued keys or other entry devices are regularly inventoried.	1) Observe practices for safeguarding keys, badges, and other devices.	• PE-3
	• AC-6.4.7: Entry codes are changed periodically.	1) Review documentation of entry code changes.	• PE-3

	• AC-6.4.8: All deposits and withdrawals of storage media from the library are authorized and logged.	1) Review procedures for the removal and return of storage media to and from the library. 2) 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.	• MP-4, • MP-CMS-1
	• AC-6.4.9: Documents/equipment are appropriately stored and are subject to maintenance and accountability procedures.	1) Examine and verify maintenance and accountability procedures for storage of documents and equipment.	• MA-1,MA-2, • MP-1,MP-2, • PE-2, PE-3, • PE-8
	• AC-6.4.10: Critical systems have emergency power supplies (for example, all alarm systems, monitoring devices, entry control systems, exit lighting, communication systems).	1) Verify that critical systems, (e.g., alarm systems, monitoring devices, entry control systems, exit lighting, and communication systems) have emergency power supplies. Identify back up systems and procedures and determine the frequency of testing. Review testing results.	• PE-11, • PE-12
• AC-6.5: Adequately protect against emerging threats, based on risk.	• AC-6.5.1: Appropriate plans have been developed and controls implemented based on a risk assessment such as a shelter in place plan and/or evacuation plan for a potential CBR attack. [A plan is in place and tested to respond to emerging threats such as a CBR attack (e.g. an appropriate shelter in place and/or evacuation plan.)	1) Interview officials, review planning documents, and related test results. Observe and document the controls in place to mitigate emerging threats.	• PE-1
	• AC-6.5.2: Outdoor areas such as air intakes, HVAC return air grilles, and roofs have been secured by restricting public access and relocating or protecting critical entry points (for example, air intake vents, protective grills, etc.)	1) Observe location of these devices and identify security measures that have been implemented.	• PE-1
	• AC-6.5.3: All outdoor air intakes are monitored by CCTV, security lighting, and/or intrusion detection sensors.	1) Verify that all outdoor air intakes are monitored by CCTV or other similar security.	• PE-1
	• AC-6.5.4: The ventilation and air filtration system has been evaluated for vulnerabilities to CBR agents and remedial action taken based on cost and risks.	1) Interview officials and review the results of any evaluations.	• PE-1

- **Configuration Management (CM)**
- CM-1: Develop and document CM policies, plans, and procedures.

• CM-1.1: CM policies, plans and procedures have been developed, documented, and implemented.	• CM-1.1.1: An effective configuration management process is documented and implemented, including: • a CM plan that identifies roles, responsibilities, procedures, and documentation requirements; • guidance that is appropriate for personnel with varying levels of skill and experience; • trained personnel who are familiar with the organization's configuration management process; • permitting only essential capabilities and restricting the use of dangerous functions, ports, protocols, and services; • regular review and approval of configuration changes by management (for example, Configuration Control Board); • appropriate representation on CCB from across the entity; • a formal SDLC methodology that includes system-level security engineering principles to be considered in the design, development, and operation of an information system. • appropriate systems documentation.	1) Review CM policies, plans, and procedures to identify roles, responsibilities, procedures, and documentation requirements. 2) Determine if a CCB exists and is operating effectively. 3) Review organizational chart to ensure that the CCB has appropriate representation services from across the entity. 4) Interview staff and review training records. 5) Interview hardware and software managers to identify the currency and completeness of CM policies, plans, procedures, and documentation. 6) Review CM documentation and test whether recent changes are incorporated. 7) Review the SDLC methodology and ensure that security is adequately considered throughout the life cycle. 8) Review a selection of system documentation to verify that the SDLC methodology was followed and complies with appropriate guidance, such as NIST SP 800-64 and SP 800-27.	• CM-1, SA-3

- CM-2: Maintain current configuration identification information.

• CM-2.1: Current configuration identification information is maintained.	• CM-2.1.1: A current and comprehensive baseline inventory of hardware, software, and firmware is documented, backed up, and protected. Information system documentation describes security controls in sufficient detail to permit analysis and testing of controls. For Federal entities, baseline meets minimum configuration management standards as required by NIST standards and OMB.	1) Request an inventory of all computer assets and determine if the inventory is accurate, complete, and whether duplicate copies are adequately protected. Select items in the inventory and trace to the asset and verify that the configuration (model, settings, etc.) is accurate. Select assets at the entity and verify that they are accurately recorded in the inventory. (Note: Selections should be focused on areas that are	• CM-8, SA-5

		most relevant to the audit.)	
	• CM-2.1.2: Hardware, software, and firmware are mapped to application it supports.	1) Determine whether management has mapped the hardware, software and firmware to the application it supports.	• CM-8, SA-5
	• CM-2.1.3: Configuration settings optimize the system's security features.	1) Determine if key component security settings conform with NIST SP 800-70 and vendor recommendations.	• CM-2, CM-6
• CM-3: Properly authorize, test, approve, track and control all configuration changes.			
• CM-3.1: All configuration changes are properly managed (authorized, tested, approved, and tracked).	• CM-3.1.1: An appropriate formal change management process is documented.	1) Where appropriate, these audit procedures should be applied to both internal and external developers and coordinated with section SM-7. (Ensure that activities performed by external third parties are adequately secure.) 2) Review the change management methodology for appropriateness. 3) Review system documentation to verify that the change management methodology was followed.	• CM-3, SA-2, • SA-3, SA-4, • SA-5, SA-10
	• CM-3.1.2: Configuration changes are authorized by management. Configuration management actions are recorded in sufficient detail so that the content and status of each configuration item is known and previous versions can be recovered.	1) Review system logs for configuration changes. Determine whether these changes have been properly authorized. 2) Examine a selection of CM and software change request forms for approvals and sufficiency of detail. 3) Interview CM management and software development staff 4) Review a selection of configuration exceptions identified by the entity in its configuration audit (Refer to CM-4.1) or through other audit procedures to identify any weaknesses in the entity's configuration change process.	• CM-3, SA-10
	• CM-3.1.3: Relevant stakeholders have access to and knowledge of the configuration status of the configuration items.	1) Interview users and ensure that they have ready access to software change requests, test reports, and configuration items associated with the various baselines being managed.	• CM-3
	• CM-3.1.4: Detailed specifications are prepared by the programmer and reviewed by	1) For the software change requests selected for	• CM-3,SA-3,

a programming supervisor for system and application software changes.	control activity CM-3.1.2: • review specifications and related documentation for evidence of supervisory review.	• SA-5
• CM-3.1.5: Test plan standards have been developed for all levels of testing that define responsibilities for each party (for example, users, system analysts, programmers, auditors, quality assurance, library control).	1) Review test plan standards.	• CM-3,SA-4, • SA-11
• CM-3.1.6: Test plans are documented and approved that define responsibilities for each party involved (for example, users, systems analysts, programmers, auditors, quality assurance, library control). • CM-3.1.7: Test plans include appropriate consideration of security. • CM-3.1.8: Unit, integration, and system testing are performed and approved in accordance with the test plan and apply a sufficient range of valid and invalid conditions. • CM-3.1.9: A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing. • CM-3.1.10: Live data are not used in testing of program changes, except to build test data files. • CM-3.1.11: Test results are documented and appropriate responsive actions are taken based on the results. • CM-3.1.12: Program changes are moved into production only when approved by management and by persons independent of the programmer.	• Perform the following procedures to determine whether control techniques CM-3.1.6 through 3.1.12 are achieved. 1) For the software change requests selected for control activity CM-3.1.2: • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and- review updated documentation. 2) Determine whether operational systems experience a high number of system failures (for example, bends) and, if so, whether they indicate inadequate testing before implementation. 3) Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.	• For CM-3.1.6: • CM-3, SA-8, • SA-11 • • For CM-3.1.7: • SA-11 • • For CM-3.1.8: • CM-3, SA-3, • SA-11 • • For CM-3.1.9: • SA-3, SA-8, • SA-11 • • For CM-3.1.10: • SA-3, SA-8 • • For CM-3.1.11: • CM-3, SA-11

		• • For CM-3.1.12: • CM-3
• CM-3.1.13: Standardized procedures are used to distribute new software for implementation.	1) Examine procedures for distributing new software.	• CM-3

• CM-3.1.14: Appropriate tools (for example, library mgt. software and manual techniques) are used to: • produce audit trails of program changes, • maintain program version numbers, • record and report program changes, • maintain creation/date information for production modules, • maintain copies of previous versions, and • control concurrent updates.	1) Review pertinent policies and procedures. 2) Interview personnel responsible for appropriate tools and library control. 3) Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. 4) Determine whether documentation is maintained on program changes, program version numbers, creation/date information, and copies of prior versions. 5) Review procedures for controlling concurrent updates. 6) Assess the adequacy of access controls over CM tools (e.g., library management software) to ensure segregation of duties is adequately enforced. (Coordinate with audit procedures in AC-4.1).	• CM-3
• CM-3.1.15: Configuration/software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.	1) For the software change requests selected for control activity CM-3.1.2: • trace changes from authorization to the final approved code; and • trace changes back from code to design specifications and functional requirements.	• CM-3, SA-3, • SA-8

• CM-3.1.16: Program development and maintenance, testing, and production programs are maintained separately (for example, libraries) and movement between these areas is appropriately controlled, including appropriate consideration of segregation of duties (see the Segregation of Duties control area.	1) Review pertinent policies and procedures and interview library control personnel. 2) Examine libraries in use. Test access to program libraries by examining security system parameters. 3) Review program changes procedures for adherence to appropriate segregation of duties between application programming and movement of programs into production. 4) 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 to ensure that unauthorized changes were not made to the programs.	• CM-3, CM-4, • SA-2, SA-3
• CM-3.1.17: Access to all programs, including production code, source code, and extra program copies, are adequately protected.	1) For critical software production programs, determine whether access control software rules are clearly defined. 2) Test access to program libraries by examining security system parameters.	• AC-3, CM-5, • CM-7
• CM-3.1.18: Configuration changes to network devices (for example, routers and firewalls) are properly controlled and documented.	1) Review a sample of configuration settings to key devices and determine if configuration changes are adequately controlled and documented.	• CM-2, CM-5, • CM-6
• CM-3.1.19: Clear policies restricting the use of personal and public domain software and prohibiting violations of software licensing agreements have been developed and are enforced.	1) Review pertinent policies and procedures. Interview users and data processing staff. Review and test management enforcement process.	• SA-6, SA-7

• CM-4: Routinely monitor the configuration.			
• CM-4.1: The configuration is routinely audited and verified.	• CM-4.1.1: Routinely validate that the current configuration information is accurate, up-to-date, and working as intended for networks, operating systems, and infrastructure applications.	1) Identify the standards and procedures used to audit and verify the system configuration. Determine when and how often the configuration is verified and audited. 2) Review a sample of the configuration verifications and audits for compliance with applicable standards. Verify that vendor-supplied system software is still supported by the vendor. 3) Evaluate adequacy of the configuration audits based on the results of the IS control audit tests performed.	• CM-4, CM-5, • SI-6, SI-7
	• CM-4.1.2: The verification and validation criteria for the configuration audit is appropriate and specifies how the configuration item will be evaluated in terms of correctness, consistency, necessity, completeness, and performance.	1) Review evaluation criteria for the selected releases to determine whether verification and validation criteria for configuration audit addresses the correctness, consistency, necessity, completeness, and performance of the configuration items. Identify all configuration items, deviations and waivers, and the status of tests. Determine if configuration items have gaps in the documentation or if there are defects in the change management process.	• CM-4, CM-5, • SI-6, SI-7
	• CM-4.1.3: Confirm compliance with applicable configuration management policy, plans, standards, and procedures.	1) Compare configuration policy, plans, standards, and procedures with observations.	• CM-4, CM-5, • SA-10, SI-7
	• CM-4.1.4: The information system periodically verifies the correct operation of security functions—on system start up and restart, on command by user with appropriate privilege—(providing system audit trail documentation) and takes appropriate action (for example, notifies system administrator, shuts the system down, restarts the system) when anomalies are discovered.	1) Interview officials and review related system documentation. Observe or test this system capability to determine that procedures are followed and related system documentation is generated and reviewed by entity security staff.	• SI-6

- CM-5: Update software on a timely basis to protect against known vulnerabilities.

• CM-5.1: Software is promptly updated to protect against known vulnerabilities.	• CM-5.1.1: Information systems are scanned periodically to detect known vulnerabilities.	1) Interview entity officials. Identify the criteria and methodology used for scanning, tools used, frequency, recent scanning results, and related corrective actions. 2) Coordinate this work with the AC section.	• RA-5, SI-3, • SI-8
	• CM-5.1.2: An effective patch management process is documented and implemented, including: • identification of systems affected by recently announced software vulnerabilities; • prioritization of patches based on system configuration and risk; • appropriate installation of patches on a timely basis, including testing for effectiveness and potential side effects on the agency's systems; and • verification that patches, service packs, and hotfixes were appropriately installed on affected systems.	1) Review pertinent policies and procedures. 2) Interview users and data processing staff.	• SI-2, SI-5
	• CM-5.1.3: Software is up-to-date; the latest versions of software patches are installed.	1) Compare vendor recommended patches to those installed on the system. If patches are not up-to-date, determine why they have not been installed.	• CM-2, MA-1, • SI-3, SI-5, • SI-8
	• CM-5.1.4: An effective virus, spam, and spyware protection process is documented and implemented, including: • appropriate policies and procedures; • effective protection software is installed that identifies and isolates suspected viruses, spam, and spyware; and • virus, spam, and spyware definitions are up-to-date.	1) Review pertinent policies and procedures. 2) Interview users and data processing staff. 3) Verify that actual software is installed and up-to-date.	• RA-5, SI-3, • SI-8
	• CM-5.1.5: The entity: (1) establishes usage restrictions and implementation guidance for IPv6 technology based on the potential to	1) Review policies and procedures for IPv6. Determine if known security vulnerabilities are mitigated by appropriate protective measures.	• SA-6, SC-1

	cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of IPv6 within the information system. Appropriate organizational officials authorize the use of IPv6.		
	• CM-5.1.6: The entity: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.	1) Review policies and procedures for VoIP. Determine if security considerations in NIST SP 800-58 are used in the information system.	• SC-19
	• CM-5.1.7: Noncurrent software releases are adequately secure, given the risk.	1) Review pertinent policies and procedures. 2) Interview users and data processing staff.	• CM-3, PL-3, • RA-4
	• CM-5.1.8: Appropriate software usage controls (software restrictions, user-installed software) are implemented and exceptions are identified.	1) Assess the adequacy of software usage controls.	• SA-6, SA-7
• CM-6: Appropriately document and approve emergency changes to the configuration.			
• CM-6.1: Adequate procedures for emergency changes are documented and implemented.	• CM-6.1.1: Appropriately document and implement procedures for emergency changes.	1) Review procedures to determine whether they adequately address emergency change requirements.	• CM-3, SA-10
• CM-6.2: Emergency changes to the configuration are documented and approved.	• CM-6.2.1: Appropriately document and approve emergency changes to the configuration and notify appropriate personnel for analysis and follow-up.	1) For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.	• CM-3, SA-10

- **Segregation of Duties (SD)**
- 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-1.1.1: Policies and procedures for segregating duties exist and are up-to-date.	1) Review pertinent policies and procedures. 2) Interview selected management and information security personnel regarding segregation of duties.	• AC-5, PS-2, • PS-6
	• SD-1.1.2: Distinct system support functions are performed by different individuals, including: • information security management • systems design • applications programming • systems programming • quality assurance/testing • library management/change management • computer operations • production control and scheduling • data control • data security • data administration • network administration • configuration management	1) Review an entity organization chart showing information security functions and assigned personnel. 2) Interview selected personnel and determine whether functions are appropriately segregated. 3) Determine whether the chart is current and each function is staffed by different individuals. 4) Review relevant alternate or back up assignments and determine whether the proper segregation of duties is maintained. 5) Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.	• AC-5, PS-2, • PS-6

• SD-1.1.3: No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual: • data entry and verification of data • data entry and its reconciliation to output • input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information) • data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval)	1) Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions. 2) Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.	• AC-5
• SD-1.1.4: Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	1) Interview management, observe activities, and test transactions. Note: Perform this in conjunction with SD-2.2.	• AC-5, AC-13, • PS-2, PS-6, • PS-7
• SD-1.1.5: Data processing personnel are not users of information systems. They and security managers do not initiate, input, or correct transactions.	1) Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.	• AC-5, PS-2, • PS-6
• SD-1.1.6: Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	1) Review the adequacy of documented operating procedures for the data center.	• AC-5, PS-2, • SA-5
• SD-1.1.7: Access controls enforce segregation of duties.	1) Audit procedures are found in section AC-3.1, but this item is listed here as a reminder. Logical and physical access controls should enforce segregation of duties.	• AC-5, PE-3

• SD-1.2: Job descriptions have been documented.	• SD-1.2.1: Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	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.	• AC-5
	• SD-1.2.2: Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	1) Review job descriptions and interview management personnel to determine if all job positions have documented technical knowledge, skills, and ability requirements that can be used for hiring, promoting, and performance evaluations.	• AC-5
• SD-1.3: Employees understand their duties and responsibilities.	• SD-1.3.1: All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	1) Interview personnel filling positions for the selected job descriptions (see SD-1.2). 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.	• AC-5
	• SD-1.3.2: Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	1) Determine from interviewing personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.	• PS-2, SA-2
	• SD-1.3.3: Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	1) Interview management personnel in these activities.	• AC-5, PS-2, • PS-6

• SD-2: Control personnel activities through formal operating procedures, supervision, and review.			
• SD-2.1: Formal procedures guide personnel in performing their duties.	• SD-2.1.1: Detailed, written instructions exist and are followed for the performance of work. • SD-2.1.2: Instruction manuals provide guidance on system operation. • SD-2.1.3: Application run manuals provide instruction on operating specific applications.	1) Perform the following procedures for SD-2.1.1 to SD-2.1.3. 2) Review manuals to determine whether formal procedures exist to guide personnel in performing their work. 3) Interview supervisors and personnel. 4) Observe processing activities.	• CM-2, SA-5
• SD-2.2: Active supervision and review are provided for all personnel.	• SD-2.2.1: Personnel are provided adequate supervision and review, including each shift for computer operations.	1) Interview supervisors and personnel. 2) Observe processing activities.	• AC-13, PS-2, • PS-6
	• SD-2.2.2: Access authorizations are periodically reviewed for incompatible functions.	1) Review sample of access authorizations for incompatible functions and evidence of supervisory review.	• AC-2, AC-5, • AC-13
	• SD-2.2.3: Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (for example, periodic risk assessments).	1) Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. 2) Note: This audit step should be performed in conjunction with audit steps in critical elements SM-2 (Periodically assess and validate risks) and SM-5 (Monitor the effectiveness of the security program).	• AC-5, RA-4
	• SD-2.2.4: Staff performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	1) Interview management and subordinate personnel. 2) Select documents or actions requiring supervisory review and approval for evidence of such performance (for example, approval of input of transactions, software changes).	• PS-1, PS-8, • PS-CMS-1
	• SD-2.2.5: Supervisors routinely review user activity logs for incompatible actions and investigate any abnormalities.	1) Interview supervisors and review user activity logs for incompatible actions. Check for evidence of supervisory review.	• AC-13

- **Contingency Planning (CP)**
- CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources.

• CP-1.1: Critical data and operations are identified and prioritized.	• CP-1.1.1: The entity categorizes information systems in accordance with appropriate guidance, such as FIPS 199, and documents the results in the system security plan.	1) Review the policies and methodology used to categorize systems and create the critical operations list. This list should identify each system and its criticality in supporting the agency's primary mission or business functions. 2) Review how systems are categorized and the critical operations list. Determine if the justifications have been documented and that they (1) prioritize data and operations by primary mission or business functions; (2) are approved by senior management; and (3) reflect current operating conditions, including key system interdependencies.	• RA-2
	• CP-1.1.2: A list of critical operations and data has been documented that • identifies primary mission or business functions, • prioritizes data and operations, • is approved by senior program managers, and • reflects current conditions including system interdependencies and technologies.	1) Determine if technology supporting critical operations is identified and appropriately considered in processing priorities. 2) Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of priorities established.	• CP-2, PL-2, • RA-3

• CP-1.2: Resources supporting critical operations are identified and analyzed.	• CP-1.2.1: Resources supporting critical operations and functions have been identified and documented. Types of resources identified should include • computer hardware, • computer software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources.	1) Interview program and security administration officials responsible for developing the critical operations listing. 2) Review documentation supporting the critical operations listing to verify that the following resources have been identified for each critical operation: • computer hardware and software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources. 3) Appropriate documentation may include contingency-related plans in NIST SP 800-34.	• CP-2
	• CP-1.2.2: Critical information technology resources have been analyzed to determine their impact on operations if a given resource were disrupted or damaged. This analysis should evaluate the impact of the outages over time and across related resources and dependent systems.	1) Determine if a current business impact analysis has been conducted that identifies critical information technology resources, disruption impacts, allowed outage times, and recovery priorities.	• RA-3
• CP-1.3: Emergency processing priorities are established.	• CP-1.3.1: Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	1) Review related policies, plans, and procedures for emergency processing and ensure: • recovery priorities have been developed, • management has approved priorities, and • priorities are documented. 2) Request a copy of the continuity of operations plan. 3) Interview program and security administration officials to determine whether they are aware of all policies and procedures for emergency processing priorities and maintain copies of the continuity of operations plan.	• CP-1, CP-2, RA-2

• CP-2: Take steps to prevent and minimize potential damage and interruption.			
• CP-2.1: Information system back up and recovery procedures have been implemented.	• CP-2.1.1: Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	1) Review written policies and procedures for backing up and transporting files. Determine how often files are backed up and rotated off site, retention periods, and security involved in transport. 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 if backup files are created and rotated off-site as prescribed and are sent before prior versions are returned. 5) Determine if the technology is implemented in such a manner as to provide appropriate availability, including consideration of backup procedures, system configuration, redundancy, environmental controls, staff training, and routine maintenance.	• CP-6, CP-9
	• CP-2.1.2: System and application documentation is maintained at the off-site storage location.	1) Locate and examine documentation.	• CP-6, CP-9, • SA-5
	• CP-2.1.3: The backup storage site is • geographically removed from the primary site (for example, not subject to the same hazards), and • protected by environmental controls and physical access controls.	1) Examine the backup storage site. Determine if there are accessibility problems between the storage and processing sites in the event of an area wide disaster.	• CP-6

	• CP-2.1.4: The information system back up and recovery procedures adequately provide for recovery and reconstitution to the system's original state after a disruption or failure including • system parameters are reset; • patches are reinstalled; • configuration settings are reestablished; • system documentation and operating procedures are available; • application and system software is reinstalled; • information from the most recent backup is available; and • the system is fully tested.	1) Interview entity officials and determine whether comprehensive procedures and mechanisms exist to fully restore the information security to its original state. 2) Determine if this recovery capability has been tested and, if so, review the test plan and test results.	• CP-2, CP-4, • CP-9, CP-10
• CP-2.2: Adequate environmental controls have been implemented.	• Common Assessment Procedures	• Audit procedures for CP-2.2 should be performed in conjunction with Section AC-6 regarding physical access controls. • • Perform the following procedures to determine whether control techniques CP-2.2.1 through 2.2.10 are achieved. 1) Examine the agency's facilities. 2) Interview site managers.	• Refer to control techniques CP-2.2.1 through 2.2.10 for related CMSRs.
	• CP-2.2.1: Fire detection and suppression devices have been installed and are working, for example, smoke detectors, fire extinguishers, and sprinkler systems.	1) 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. 2) Observe fire detection and suppression devices. 3) Determine whether the activation of heat and smoke detectors will notify the fire department.	• PE-13
	• CP-2.2.2: Controls have been implemented to mitigate other disasters, such as floods, earthquakes, terrorism, etc.	1) Review the entity's assessment of environmental risks and related controls.	• PE-9, PE-10, PE-11, PE-12, PE-13, PE-14,

			PE-15, PE-17, PE-18, RA-3
	• CP-2.2.3: Redundancy exists in critical systems (for example, power and air cooling systems)	1) Observe the operation, location, maintenance, and access to critical systems.	• PE-11, PE-14
	• CP-2.2.4: Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known.	1) Observe whether water can enter through the computer room ceiling or whether pipes are running through the facility and that there are water detectors on the floor.	• PE-15
	• CP-2.2.5: An uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shut down.	1) Observe power backup arrangements and results of testing.	• PE-11
	• CP-2.2.6: Humidity, temperature, and voltage are controlled within acceptable levels.	1) Determine whether humidity, temperature, and voltage are appropriately controlled.	• PE-9, PE-10, • PE-14, PE-15
	• CP-2.2.7: Emergency lighting activates in the event of a power outage and covers emergency exits and evacuation routes.	1) Observe that emergency lighting works and that power and other cabling is protected.	• PE-12
	• CP-2.2.8: A master power switch or emergency shut-off switch is present and appropriately located.	1) Observe power shut-off arrangements.	• PE-10
	• CP-2.2.9: Environmental controls are periodically tested at least annually for federal agencies	1) Review test policies. 2) Review documentation supporting recent tests of environmental controls and follow-up actions.	• PE-1, PE-9, • PE-10, PE-11, • PE-12, PE-13, • PE-14, PE-15
	• CP-2.2.10: Eating, drinking, and other behavior that may damage computer equipment is prohibited.	1) Review policies and procedures regarding employee behavior. 2) Observe employee behavior.	• PL-4
• CP-2.3: Staff have been trained to respond to	• CP-2.3.1: Operational and support personnel have received training and understand their emergency roles and responsibilities.	1) Interview security personnel and appropriate operational and support staff and ensure that they understand their roles and responsibilities.	• CP-3
	• CP-2.3.2: Personnel receive periodic	1) Review training records and training course	• PE-13, PE-

emergencies.	environmental controls training including emergency fire, water, and alarm incident procedures. • CP-2.3.3: Emergency response procedures are documented. • CP-2.3.4: Emergency procedures are periodically tested.	documentation. Determine whether all personnel have received up-to-date training and that the scope of the training is adequate. 1) Review emergency response procedures for completeness and determine whether roles and responsibilities are clearly defined. 1) Review test policies. 2) Review test documentation. 3) Interview operational and data center staff.	14, • PE-15 • PE-13, PE-14, • PE-15 • PE-1, PE-13, • PE-14, PE-15
• CP-2.4: Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	• CP-2.4.1: Policies and procedures exist and are up-to-date. • CP-2.4.2: Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations. • CP-2.4.3: Regular and unscheduled maintenance performed is documented. • CP-2.4.4: Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance. • CP-2.4.5: Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	1) Review policies and procedures. • Perform the following procedures to determine whether control techniques CP-2.4.2 through CP-2.4.4 are achieved. 1) Interview information security, data processing, and user management. 2) Review maintenance documentation. 3) Determine when maintenance is performed, if it is in accordance with vendor specifications, and if there is minimal impact on system availability. 1) Interview information security and data center management.	• CM-1, IR-1, • MA-1, MA-3, • MA-5, SI-1 • For CP-2.4.2 • MA-2, MA-6 • • For CP-2.4.3 • MA-2 • • For CP-2.4.4 • MA-2 • CP-2, CP-7, • CP-8, MA-6

• CP-2.4.6: Goals are established by senior management on the availability of data processing and on-line services. • CP-2.4.7: Records are maintained on the actual performance in meeting service schedules. • CP-2.4.8: Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	• Perform the following procedures to determine whether control techniques CP-2.4.6 through CP-2.4.8 are achieved. 1) Interview senior management, information security management, data processing management, and user management. 2) Review supporting documentation, including system performance metrics.	• For CP-2.4.6 • PL-2, RA-3, • SA-5 • • For CP-2.4.7 • PL-2, SA-5 • • For CP-2.4.8 • MA-2, SA-5
• CP-2.4.9: Senior management periodically reviews and compares the service performance achieved with the goals and surveys of user departments to see if their needs are being met.	1) Interview senior management, information security management, data processing management, and user management. 2) Review supporting documentation such as user surveys, service goals, metrics measuring system availability, service schedules, and test plans.	• SA-5
• CP-2.4.10: Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing. • CP-2.4.11: Advance notification of hardware changes is given to users so that service is not unexpectedly interrupted.	1) For control techniques CP-2.4.10 and CP-2.4.11, review supporting documentation for scheduling of hardware changes, including staff notifications.	• For CP-2.4.10 • CM-3, MA-2, • SA-10 • • For CP-2.4.11 • MA-2

• CP-3: Develop and document a comprehensive contingency plan.			
• CP-3.1: An up-to-date contingency plan is documented.	• CP-3.1.1: A contingency plan has been documented that • is based on clearly defined contingency planning policy; • reflects current conditions, including system interdependencies; • is approved by key affected groups, including senior; information security; and data center management, and program managers; • clearly assigns recovery responsibilities; • includes detailed instructions for restoring operations (both operating system and critical applications) • identifies the alternate processing facility and the back up storage facility; • includes procedures for when data/service center is unable to receive or transmit data; • identifies critical data files; • is detailed enough to be understood by all entity managers; • includes telecommunications and computer hardware compatible with the agency's needs; • includes necessary contact numbers; • includes system-recovery instructions; • was distributed to all appropriate personnel; and • was coordinated with related plans and activities.	1) Review contingency planning policy and determine if it documents the agency's overall contingency objectives and establishes the organizational framework and responsibilities for contingency planning. 2) Obtain contingency plans (see NIST SP 800-34) and compare their provisions with the most recent risk assessment and with a current description of automated operations. 3) Compare the contingency plans to security-related plans, facility-level plans, and agency/entity-level plans such as those in NIST contingency planning guidance. 4) Determine if the contingency plans include • appropriate consideration of the technology, including alternative processing requirements, • recovery of the security infrastructure, and • interdependencies with other systems (i.e., other component, federal, state, or local agencies) that could affect the contingency operations.	• CP-1, CP-2, • CP-5, CP-7, • CP-8, CP-10
	• CP-3.1.2: Contingency plans are reevaluated before proposed changes to the information system are approved to determine if major modifications have security ramifications that require operational changes in order to	1) Interview senior management, information security management, and program managers.	• CP-5, SA-3

	maintain adequate risk mitigation.		
	• CP-3.1.3: Procedures allow facility access in support of restoration of lost information under the contingency plans in the event of an emergency.	1) Determine whether emergency and temporary access authorizations are properly approved, documented, controlled, communicated, and automatically terminated after a predetermined period. 2) These procedures should be performed in conjunction with Section AC-3.1.8 and AC-6.1.8 regarding access controls.	• CP-2, CP-10
	• CP-3.1.4: The plan provides for backup personnel so that it can be implemented independent of specific individuals.	1) Review the contingency plan.	• CP-2
	• CP-3.1.5: User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.	1) Interview senior management, information security management, and program managers.	• CP-2
	• CP-3.1.6: Several copies of the current contingency plan are securely stored off-site at different locations.	1) Observe copies of the contingency and related plans held off-site.	• CP-2, CP-5, • CP-6
	• CP-3.1.7: The contingency plan is periodically reassessed and revised as appropriate. At a minimum, the plan is reassessed when there are significant changes in entity mission, organization, business processes, and IT infrastructure (e.g. hardware, software, personnel).	1) Review the plan and any documentation supporting recent plan reassessments.	• CP-5
• CP-3.2: Arrangements have been made for alternate data processing, storage, and telecommunicat	• CP-3.2.1: Contracts or interagency agreements have been established for backup processing facilities that • are in a state of readiness commensurate with the risks of interrupted operations, • have sufficient processing and storage capacity, and • are likely to be available for use.	1) Interview officials and review contracts and agreements including processing priorities for the backup site. Determine if the back up site is properly configured and ready to be used as an operational site.	• CP-7

ions facilities.	• CP-3.2.2: Alternate network and telecommunication services have been arranged.	1) Interview officials and review contracts and agreements including the priority of service provisions for the backup service provider. 2) Determine if the backup service provides separate failure points and is geographically removed from the primary provider.	• CP-8
	• CP-3.2.3: Arrangements are planned for travel, lodging, and protection of necessary personnel, if needed.	1) Interview officials and review the plan.	• CP-2, CP-10
• CP-4: Periodically test the contingency plan and adjust it as appropriate.			
• CP-4.1: The plan is periodically tested.	• CP-4.1.1: The contingency plan is periodically tested under conditions that simulate a disaster. Disaster scenarios tested may be rotated periodically. Typically, contingency plans are tested annually or as soon as possible after a significant change to the environment that would alter the assessed risk.	1) Review testing policies and methodology used to select disaster scenarios. Determine when and how often contingency plans are tested. 2) Determine if technology is appropriately considered in periodic tests of the contingency plan and resulting adjustments to the plan. Review test results. 3) Observe a disaster recovery test.	• CP-4, CP-10
• CP-4.2: Test results are analyzed and the contingency plan is adjusted accordingly.	• CP-4.2.1: Test results are documented and a report, such as a lessons learned report, is developed and provided to senior management.	1) Review final test report. 2) Interview senior managers to determine if they are aware of the test results.	• CP-4
	• CP-4.2.2: The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	1) Review any documentation supporting contingency plan adjustments.	• CP-5

APPENDIX II: CFO BUSINESS PROCESS APPLICATION LEVEL CONTROLS TESTING PROCEDURES

Business Process Application Level Controls include the general controls applied at the business process application level (also referred to as application security) as well as the three categories of business process application controls. These are those controls over the completeness, accuracy, validity, confidentiality and availability of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of entitywide and system level general controls

• Control Activity	• Control Techniques	• Assessment Procedures	• Related CMSR
• **Application Level General Controls (AS)**			
• AS-1: Implement effective application security management.			
• AS-1.1: A comprehensive application security plan is in place.	• AS-1.1.1: A comprehensive application security plan has been developed and documented. Topics covered include: • Application identification and description • Application risk level • Application owner • Person responsible for the security of the application • Application interconnections / information sharing • A description of all of the controls in place or planned, including how the controls are, or will be, implemented and special considerations • Approach and procedures regarding security design and upgrade process • Process for developing security roles • General security administration policies, including ongoing security role maintenance and development • Identification of sensitive transactions in	1) Inspect the application security plan to determine whether it adequately addresses all of the relevant topics.	• PL-2, SA-5, • SA-10, SA-11

each functional module • Identification of high risk segregation of duty cases • Roles and responsibilities of the security organization supporting the system with consideration to segregation of duties • Security testing procedures • Coordination with entitywide security policies • Procedures for emergency access to the production system, including access to update programs in production, direct database updates, and modification of the system change option • System parameter settings, compliant with entitywide agency policies • Access control procedures regarding the use of system delivered critical user IDs		
• AS-1.1.2: Sensitive accounts are identified for each business process or sub-process, and appropriate security access privileges are defined and assigned.	1) Review the entity's identification of sensitive transactions for the business process being audited for appropriateness and completeness. 2) Observe and inspect procedures for identifying and assigning sensitive activities. 3) Inspect authorizations for sensitive activities.	• AC-3, SA-5
• AS-1.1.3: Access privileges are developed to prevent users from executing incompatible transactions within the application via menus or screens.	1) Through inquiry and inspection, determine whether the application security plan includes plans to identify segregation of duty conflicts in each of the business processes under assessment (master data and transaction data; data entry and reconciliation), and addresses controls to mitigate risks of allowing segregation of duty conflicts in a user's role.	• AC-5, SA-5

• AS-1.2: Application security risk assessments and supporting activities are periodically performed.	• AS-1.2.1: Security risks are assessed for the applications and supporting systems on a periodic basis or whenever applications or supporting systems significantly change. The risk assessments and validation, and related management approvals, are documented and maintained. The risk assessments are appropriately incorporated into the application security plan.	1) Obtain the most recent security risk assessment for each application under assessment. 2) Inspect the risk assessments to determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by testing. Consider compliance with FISMA, OMB, NIST, and other requirements/guidance and whether technology and business processes are appropriately considered in the risk assessment. 3) Obtain and inspect the relevant application security plan(s) to determine whether the risk assessments are appropriately incorporated into the application security plan.	• PL-2, PL-3, • RA-3, RA-4 •
• AS-1.3: Policies and procedures are established to control and periodically assess access to the application.	• AS-1.3.1: Business process owners accept risks and approve the policies and procedures.	1) Determine through interview with entity management whether policies and procedures have been established to review access to the application.	• CA-4
	• AS-1.3.2: Policies and Procedures are: • documented • appropriately consider business process security needs. • appropriately consider segregation of application user activity from the system administrator activity.	1) Review policies and procedures to determine whether they have appropriately considered (1) business security needs and (2) segregation of application user activity from system administrator activity.	• AC-1, AC-5, • AT-1, AU-1, • CA-1, CM-1, • CP-1, IA-1, • IR-1, MA-1, • MP-1, PE-1, • PL-1, PS-1, • RA-1, SA-1, • SC-1, SI-1

• AS-1.4: Application owners and users are aware of application security policies.	• AS-1.4.1: The entity has an effective process to communicate application security policies to application owners and users and reasonably assure that they have an appropriate awareness of such policies.	1) Obtain an understanding of how application owners and users are made aware of application security policies and assess the adequacy of the process. 2) Interview selected application owners and users concerning their awareness of application security policies.	• AC-1, AT-1, • AU-1, CA-1, • CM-1, CP-1, • IA-1, IR-1, • MA-1, MP-1, • PE-1, PL-1, • PS-1, RA-1, • SA-1, SC-1, • SI-1
•	• AS-1.4.2: Personnel policies related to the application appropriately address security and application owners and users have adequate training and experience.	1) Review personnel policies for appropriateness and consistency with entitywide policies. Assess the adequacy of training and expertise for application owners and users. 2) Assess the adequacy of training and expertise for application owners and users.	• AT-1, AT-3, • AT-4, PS-1
• AS-1.5: Management periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	• AS-1.5.1: An application security policy and procedure test plan is developed and documented.	1) Inquire of management, and inspect testing policies and procedures.	• SA-11
	• AS-1.5.2: Security controls related to each major application are tested at least annually.	1) Inspect the overall testing strategy, a sample of test plans and related testing results. 2) Determine if the scope of testing complies with OMB Circular A-123 Revised (federal entities) and other appropriate guidance. 3) Determine if C&A testing is performed that complies with FISMA and NIST requirements.	• CA-2, CA-7, • SA-5, SA-11
	• AS-1.5.3: The frequency and scope of testing is commensurate with the risk and criticality of the application to the agency's mission.	1) Based upon the application test plan, assess whether the frequency and scope of testing is appropriate, given the risk and critically of the application.	• CA-2
	• AS-1.5.4: Compliance, and a report on the state of compliance, is part of the entity's security program.	1) Determine through inquiry and inspection if the application security plan is incorporated into the entity's security program.	• CA-4

• AS-1.6: Management effectively remediates information security weaknesses.	• AS-1.6.1: Management has a process in place to correct deficiencies.	1) Inquire of management and inspect security polices and procedures, including assessment and resolution plan.	• CA-5
	• AS-1.6.2: Management initiates prompt action to correct deficiencies. Action plans and milestones are documented and complete.	1) Inspect recent FMFIA/A-123 and POA&M (or equivalent) reports for reasonableness of corrective actions (nature and timing),. 2) Determine whether application security control deficiencies (identified by the audit, by management testing, and by others) are included in the plans of action and milestones (or equivalent). and determine the status of corrective actions	• CA-5
	• AS-1.6.3: Deficiencies are analyzed by application (analysis may be extended to downstream, upstream, and other related applications), and appropriate corrective actions are applied.	1) Evaluate the scope and appropriateness of planned corrective actions through inquiry of management and inspection of evidence.	• CA-5
	• AS-1.6.4: Corrective actions are tested after they have been implemented and monitored on a continuing basis.	1) Inspect documentation to determine if implemented corrective actions have been tested and monitored periodically.	• CA-2, CA-7
• AS-1.7: External third party provider activities are secure, documented, and monitored.	• AS-1.7.1: Policies and procedures concerning activities of third party providers are developed and include provisions for: • application compliance with agency's security requirements, and • monitoring of compliance with regulatory requirements.	1) Inspect policies and procedures pertaining to external parties for the application under assessment. 2) Inspect documentation to determine whether the external third party provider's need to access the application is appropriately defined and documented.	• PS-6, PS-7, • SA-4, SA-9
	• AS-1.7.2: A process is in place to monitor third party provider compliance to the agency's regulatory requirements.	1) Inquire of management regarding procedures used to monitor third party providers. 2) Inspect external reports (SAS 70) or other documentation supporting the results of compliance monitoring.	• PS-7, SA-9

• AS-2: Implement effective application access controls.			
• AS-2.1: Application boundaries are adequately protected.	AS-2.1.1: Application boundaries are identified in security plans. Application boundaries are adequately secure.	1) Review security plans for proper identification of application boundaries. 2) Evaluate the effectiveness of controls over application boundaries.	• PL-2, SC-7
• AS-2.2: Application users are appropriately identified and authenticated.	• AS-2.2.1: Identification and authentication is unique to each user. All approved users should enter their user ID (unique) and password (or other authentication) to gain access to the application.	1) Inspect pertinent policies and procedures, and NIST guidance for authenticating user IDs. 2) Through inquiry, observation or inspection, determine the method of user authentication used (password, token, biometrics, etc.). 3) If a password system is used, gain an understanding of the specific information and evaluate its appropriateness, including application security authentication parameters, via inspection of system reports or observation of the system, including appropriate testing. See AC-2 for more information on criteria for evaluating password policies.	• AC-2, IA-2, • IA-4, SA-5
• AS-2.3: Security policies and procedures appropriately address ID and password management.	• AS-2.3.1: The agency has formal procedures and processes for granting users access to the application. The agency's IT security policies and procedures contain guidance for: • Assigning passwords; • Changing and resetting passwords; and • Handling lost or compromised passwords	1) Through inquiry, observation, and inspection, understand and assess procedures used by the agency for application password management: • Procedures for initial password assignment, including the password parameters; • Procedures for password changes, including initial password change; • Procedures for handling lost passwords (password resetting); and • Procedures for handling password compromise.	• IA-5

	• AS-2.3.2: The application locks the user's account after a pre-determined number of attempts to log-on with an invalid password. The application may automatically reset the user account after a specific time period (an hour or a day), or may require an administrator to reset the account. If the user is away from his/her workspace for a preset amount of time, or the user's session is inactive, the application automatically logs off the user's account.	1) After obtaining an understanding of the user authentication process, inspect and/or observe the following: • Whether access to the application is permitted only after the user enters their user ID and password. • Observe a user executing invalid logins and describe the actions taken. 2) Either 1) inspect system security settings, or 2) observe an idle user workspace to determine whether the application logs the user off after an elapsed period of idle time.	• AC-3, AC-11, • AC-12, • AC-14, • SC-10
	• AS-2.3.3: Each application user has only one user ID.	1) Through observation and inspection, determine whether each user has one, and only one, user ID to access the application	• IA-2
	• AS-2.3.4: Multiple log-ons are controlled and monitored.	1) Through inquiry, observation or inspection, determine whether the application allows multiple log-ons by the same user. If so, understand and document monitoring procedures that reasonably assure that multiple log-ons are not used to allow application access to an unauthorized user, or to violate effective segregation of duties.	• AC-10
• AS-2.4: Access to the application is restricted to authorized users.	• AS-2.4.1: Before a user obtains a user account and password for the application, the user's level of access has been authorized by a manager and the application administrator.	1) Review policies and procedures. From a sample of user accounts determine whether the user level of access was authorized by appropriate entity management.	• AC-2
	• AS-2.4.2: Owners periodically review access to ensure continued appropriateness.	1) Interview security administrators and inspect evidence of the effectiveness of periodic review of access by owners.	• AC-2

	• AS-2.4.3: Access is limited to individuals with a valid business purpose (least privilege)	1) Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed. 2) Through inquiry, observation, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how. 3) Based on the sample of users in AS-2.4.1 above, determine whether the user access is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.	• AC-6
• AS-2.5: Public access is controlled. (Based on an agency's business mission, the agency may allow the public to have access to the application.)	• AS-2.5.1: The agency implements a security plan and process for 1) identification and authorization of users; 2) access controls for limited user privileges; 3) use of digital signatures; 4) prohibition of direct access by the public to production data; and 5) compliance with NIST requirements	1) Obtain an understanding of the following controls through inquiry of the application owner, inspection of source documents, and/or observation of the following: • Identification and authentication; • Access controls for limiting user privileges(read, write, modify, delete); • Use of digital signatures; • Prohibition of direct access by the public to live databases and restricted/sensitive records; and • Legal considerations (i.e., privacy laws, OMB, NIST, etc.).	• AC-2, AC-3, • AC-6, IA-2, • PL-2, SA-5, • SC-2, SC-17
• AS-2.6: User access to sensitive transactions or	• AS-2.6.1: Owners have identified sensitive transactions or activities for the business process.	1) Inquire of responsible personnel and inspect pertinent policies and procedures covering segregation of application duties	• AC-5, SA-5

activities is appropriately controlled.	• AS-2.6.2: Owners authorize users to have access to sensitive transactions or activities.	1) Determine whether the process owners have identified a list of sensitive transactions or activities for their area. 2) Inspect the user administration procedures to determine whether they include a requirement for the process owner to approve access to transactions or activities in their area of responsibility. 3) Through inquiry and inspection, determine whether user access is authorized by process owners.	• AC-5, SA-5
	• AS-2.6.3: Security Administrators review application user access authorizations for access to sensitive transactions and discuss any questionable authorizations with owners.	1) Select a sample of user access request forms or other authorization documents [can use same sample selected in AS-2.4.1 and AS-2.4.3] and inspect them to determine whether the process owners have approved user access to appropriate transactions or activities. 2) Interview security administrators and inspect user access authorization procedures to determine whether access to sensitive transactions require approval by the process owner.	• AC-3
	• AS-2.6.4: Owners periodically review access to sensitive transactions and activities to ensure continued appropriateness.	1) Inspect evidence of periodic review by owners of access to sensitive transactions.	• AC-3
	• AS-2.6.5: Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	1) Review security software parameters and review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. 2) Obtain a list of recently terminated employees and, for a selection, determine whether system access was promptly terminated.	• AC-2

	• AS-2.6.6: Access to sensitive transactions is limited to individuals with a valid business purpose (least privilege)	1) Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed. 2) Through inquiry, observations, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how. 3) Obtain a list of users with access to identified sensitive transactions for the business process under assessment. Inspect the list to determine whether the number of users having access to sensitive transactions/activities is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.	• AC-6, SA-5
• AS-2.7: Sensitive application resources are adequately protected.	• AS-2.7.1: The entity identifies sensitive application resources. Access to sensitive application resources is restricted to appropriate users. Sensitive application data is encrypted, where appropriate.	1) Evaluate the completeness of sensitive application resources identified. 2) Assess the adequacy of IS controls over sensitive application resources. 3) Review implementation of encryption of sensitive application data, where appropriate.	• AC-3, SA-5
• AS-2.8: An effective access audit and monitoring program is in place, documented, and approved.	• AS-2.8.1: Policies and procedures are established to reasonably assure that application security audit and monitoring is effective	1) Inspect documented policies and procedures for application security administration for each application in scope. 2) Determine whether the monitoring program has built-in procedures to identify inappropriate user assignments. 3) Through inquiry and inspection, determine whether monitoring procedures are performed on a regular basis. 4) Determine whether the exceptions are handled appropriately and in a timely manner.	• AU-1, SA-5

• AS-2.9: Application security violations are identified in a timely manner.	• AS-2.9.1: Logging and other parameters are appropriately set up to notify of security violations as they occur.	1) Observe and inspect application logging and other parameters that identify security violations and exceptions. (For example, parameter set up indicates whether or not users can logon to an application more than once)	• AU-2, AU-3, • SA-5
• AS-2.10: Exceptions and violations are properly analyzed and appropriate actions taken.	• AS-2.10.1: Reportable exceptions and violations are identified and logged. Exception reports are generated and reviewed by security administration. If an exception occurs, specific action is taken based upon the nature of exception.	1) Observe and inspect management's monitoring of security violations, such as unauthorized user access. 2) Inspect reports that identify security violations. Through inquiry and inspection, note management's action taken. 3) Inspect reports of authorized segregation of duty conflicts sensitive process access; Assess business level authorization and monitoring, if applicable	• AU-6
• AS-2.11: Physical security controls over application resources are adequate.	• AS-2.11.1: Physical controls are integrated with entitywide and system-level controls. Application resources sensitive to physical access are identified and appropriate physical security is placed over them.	1) Review the appropriateness of the entity's identification of application resources sensitive to physical access. 2) Assess the adequacy of physical security over sensitive application resources.	• PE-1, PL-2
• AS-3: Implement effective application configuration management.			
• AS-3.1: Policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly.	• AS-3.1.1: Appropriate policies and procedures are established for application configuration management.	1) Inspect documented policies and procedures related to application change control procedures. 2) Through inquiry and inspection, identify key transactions that provide user access to change application functionality. 3) Inspect transaction reports of changes made to the application. For a sample of changes, inspect documentation of the changes made, including the validity, reasons, authorization, and the user authority. Note the handling of exceptions.	• CM-3, SA-10
• AS-3.2: Current	• AS-3.2.1: The entity maintains information	1) Review the entity's configuration management	• CM-6, SA-

configuration information is maintained.	on the current configuration of the application.	information.	10
• AS-3.3: A system development life cycle methodology has been implemented.	• AS-3.3.1: A SDLC methodology has been developed that • provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, • is sufficiently documented to provide guidance to staff with varying levels of skill and experience, • provides a means of controlling changes in requirements that occur over the system life, and • includes documentation requirements.	1) Review SDLC methodology. 2) Review system documentation to verify that SDLC methodology was followed.	• SA-3
• AS-3.4: Authorizations for changes are documented and maintained.	• AS-3.4.1: change request forms are used to document requests and related projects.	1) Identify recent software modification and determine whether change request forms were used.	• CM-3, SA-10
	• AS-3.4.2: Change requests must be approved by both system users and IT staff.	1) Examine a selection of software change request forms for approval.	• CM-3, SA-10

• AS-3.5: Changes are controlled as programs progress through testing to final approval.	• AS-3.5.1: Test plan standards are developed for all levels of testing that define responsibilities for each party (e.g., users, system analysis, programmers, auditors, quality assurance, library control).
	• AS-3.5.2: Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.
	• AS-3.5.3: Software changes are documented so that hey can be traced from authorization to the final approved code.
	• AS-3.5.4: Test plans are documented and approved that define responsibilities for each party involved.
	• AS-3.5.5: Unit, integration, and system testing are performed and approved
	  • in accordance with the test plan and
	  • applying a sufficient range of valid and invalid conditions.
	• AS-3.5.6: A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.
	• AS-3.5.7: Test results are reviewed and documented.
	• AS-3.5.8: Program changes are moved into production only upon documented approval from users and system development management.
	• AS-3.5.9: Documentation is updated when a new or modified system is implemented.
		• Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved.
		1) Review test plan standards.
		2) Examine a selection of recent software changes and
		  • review specifications;
		  • trace changes from code to design specifications;
		  • review test plans;
		  • compare test documentation with related test plans;
		  • analyze test failures to determine if they indicate ineffective software testing;
		  • review test transactions and data;
		  • review test results;
		  • verify user acceptance; and
		  • review updated documentation.
		3) Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.
			• For AS-3.5.1
			• SA-3
			•
			• For AS-3.5.2:
			• SA-3
			•
			• For AS-3.5.3:
			• CM-3, SA-3,
			• SA-5, SA-10
			•
			• For AS-3.5.4:
			• SA-3, SA-10,
			• SA-11
			•
			• For AS-3.5.5:
			• SA-3
			•
			• For AS-3.5.6:
			• SA-3, SA-11
			•
			• For AS-3.5.7:
			• SA-3, SA-11
			•
			• For AS-3.5.8:
			• CM-3, SA-

			10 • • For AS-3.5.9: • SA-5
• AS-3.6: Access to program libraries is restricted.	• AS-3.6.1: Separate libraries are maintained for program development and maintenance, testing, and production programs. • AS-3.6.2: Source code is maintained in a separate library.	1) Examine libraries to determine whether separate libraries are used for development and maintenance, testing, and production. 1) Verify source code exists for a selection of production code modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting	• CM-3, SA-10 • CM-3, SA-10

		module size to production load module size..	
	• AS-3.6.3: Access to all programs, including production code, source code, and extra program copies are protected by access control software and operating system features.	1) For critical software production programs, determine whether access control software rules are clearly defined. 2) Test access to program libraries by examining security system parameters.	• AC-3
• AS-3.7: Movement of programs and data among libraries is controlled.	• AS-3.7.1: A group independent of the user and programmers control movement of programs and data among libraries. Before and after images of program code are maintained and compared to ensure that only approved changes are made.	1) Review pertinent policies and procedures. 2) For a selection of program changes, examine related documentation to verify that • procedures for authorizing movement among libraries were followed, and • before and after images were compared.	• AC-5, CM-4, • SA-10
• AS-3.8: Access to application activities/ transactions is controlled via user roles (access privileges).	• AS-3.8.1: User accounts are assigned to a role in the application. Roles are designed and approved by management to provide appropriate access and prevent an unauthorized user from executing critical transactions in production that change application functionality.	1) Inspect system reports and identify users who have access to configuration transactions. 2) For a sample of users identified above, inspect user authorization forms to determine whether the user's access was authorized.	• AC-3, AC-5, • AC-6
• AS-3.9: Access to all application programs/codes and tables are controlled.	• AS-3.9.1: Changes to application programs, codes and tables are either restricted or denied in the production environment. All changes are made using the approved change control process. User access to the application programs, codes, and tables is provided only for emergency user IDs.	1) Through inquiry and inspection, identify key programs and tables for the application. 2) Inspect system reports of users with access to the key programs, codes and tables. Select a sample of users that have access to the identified programs and tables. Inspect documentation supporting how the access was provided. Note exceptions.	• CM-5, SA-10

• AS-3.10: Access to administration (system) transactions that provide access to table maintenance and program execution is limited to key users.	• AS-3.10.1: Security design includes consideration for sensitive administration (system) transactions and restricted user access to these transactions.	1) Inspect policies and procedures regarding restricted access to system administration transactions. 2) Through inquiry and inspection, identify the system administration transactions. 3) Inspect system reports of user access to these transactions. 4) Select a sample of users with administration access and inspect documentation to determine whether access was authorized. 5) Select a sample of system administration transactions executed by the system users and inspect resulting changes to the system elements, such as the program code or table. 6) Inspect critical or privileged IDs (e.g., fire call ID) to determine if activity is logged.	• AC-3
• AS-3.11: Access and changes to programs and data are monitored.	• AS-3.11.1: Procedures are established to reasonably assure that key program and table changes are monitored by a responsible individual who does not have the change authority. The procedures provide the details of reports/logs to run, specific valuation criteria and frequency of the assessment.	1) Inspect documented procedures related to monitoring change control. 2) Select a sample of reports or logs that are reviewed, and inspect to note evidence of monitoring compliance.	• CM-4
• AS-3.12: Changes are assessed periodically.	• AS-3.12.1: Periodic assessment of compliance with change management process, and changes to configurable objects and programs.	1) Inspect evidence of documented assessments performed. 2) Determine who performed the assessment and note the exception handling procedures.	• CA-2
• AS-3.13: Applications are updated on a timely manner to protect against known vulnerabilities.	• AS-3.13.1: The entity follows an effective process to identify vulnerabilities in applications and update them.	1) Determine whether vendor supplied updates have been implemented. 2) Assess management's process for identifying vulnerabilities and updating applications.	• SI-2, SI-5
• AS-3.14: Emergency application changes	• AS-3.14.1: The entity follows an effective process to properly document, test, and approve emergency changes.	1) Inspect evidence of proper documentation, testing, and approval of emergency changes.	• CM-3

are properly documented, tested, and approved.			
• AS-4: Segregate application user access to conflicting transactions and activities and monitor segregation.			
• AS-4.1: Incompatible activities and transactions are identified.	• AS-4.1.1: Owners have identified incompatible activities and transactions, and documented them on a segregation of duty matrix.	1) Through inquiry of management and inspection of policies and procedures, understand how management identifies incompatible activities and transactions.	• AC-5
	• AS-4.1.2: Owners have appropriately considered risk acceptance when allowing segregation of duty conflicts in user roles.	1) Inspect list of segregation of duty conflicts to determine whether management has identified the segregation of duty conflicts appropriate for the business process and considered risk acceptance when allowing the conflicts.	• AC-5

• AS-4.2: Application controls prevent users from performing incompatible duties.	• AS-4.2.1: Users are prevented by the application from executing incompatible transactions, as authorized by the business owners.	1) Through inquiry, observation, and inspection, determine how the application segregates users from performing incompatible duties. 2) Obtain and inspect a listing of users with access to the application. For a sample of users (can use same sample selected in AS-2.4.1, AS-2.4.3 & AS-2.6.3), inspect documentation to determine whether access to menus/screens corresponds with the user's defined duties. Evaluate whether their duties and access is appropriate to prevent employees from performing incompatible duties. 3) Specifically, perform the following steps: • Obtain a system-generated user listing for the application (and other applications, if applicable); • For a selected sample of users, inspect their access profiles to determine whether access is appropriate (e.g., users have update access); and • For the selected sample of users, inspect their access profiles to determine if any of the users have access to menus with conflicting duties.	• AC-3, AC-5
• AS-4.3: There is effective segregation of duties between the security administration function of the application and the user functions.	• AS-4.3.1: The profiles for security administrators do not have privileges to input and/or approve transactions.	1) Based on the inspection of user profiles, determine if: • individuals with security administration functions have access to input, process, or approve transactions; • security administrators have access to more than application security administration functions; and • security administrators are prevented from accessing production data.	• AC-5

• AS-4.4: User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.	• AS-4.4.1: Owners authorize users to have access to transactions or activities that cause segregation of duty conflicts only when supported by a business need.	1) Inspect user administration policy to determine whether owner approval is required to access transactions or activities in their area of responsibility. 2) Obtain and inspect a system report of users with conflicting responsibilities within the application. Obtain a sample of user access request forms (electronic documents/workflow, if applicable) and verify that the owners have approved user access to appropriate transactions or activities.	• AC-5, AC-13, • SA-5
	• AS-4.4.2: Security Administrators review application user access authorizations for segregation of duties conflicts and discuss any questionable authorizations with owners.	1) Interview security administrators and observe and inspect relevant procedures and documentation. If the security administrator's review is documented on the request form, inspect a sample of forms to note evidence of the security administrator's review.	• AC-3
	• AS-4.4.3: Owners periodically review access to identify unauthorized segregation of duties conflicts and determine whether any authorized segregation of duties conflicts remain appropriate.	1) Interview owners and inspect documentation; determine whether appropriate procedures are in place to identify and remove or modify access, as needed.	• AC-2, AC-3
• AS-4.5: Effective monitoring controls are in place to mitigate segregation of duty risks.	• AS-4.5.1: Process Owner has identified the segregation of duty conflicts that can exist, and the roles and users with conflicts.	1) Inspect documentation of roles and users with conflicts.	• AC-5, SA-5
	• AS-4.5.2: Documented monitoring controls are in place that specifically address the conflict that the control mitigates.	1) Identify segregation of duty conflicts (including those that were intentionally established by the entity) and review documentation to determine whether: • monitoring controls adequately mitigate the risks created by the segregation of duty conflict; and • monitoring controls are effective. This can be achieved by inspecting the evidence collected by management.	• AC-5, AC-13, • SA-5
	• AS-4.5.3: Management has documented evidence of monitoring of control	1) Review evidence of monitoring of control effectiveness.	• AC-13

	effectiveness.		
• AS-5: Implement effective application contingency planning.			
• AS-5.1: Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.	• AS-5.1.1: Determine the critical functions performed by the application and identify the IT resources, including key data and programs, required to perform them. • AS-5.1.2: Identify the disruption impacts and allowable outage times for the application. • AS-5.1.3: Develop recovery priorities that will help determine recovery strategies.	• Perform the following procedures for AS-5.1.1 to AS-5.1.3. 1) Review the policies and methodology, and the BIA (if conducted) used to determine the application's critical functions and supporting IT resources, the outage impacts and allowable outage times, and the recovery priorities. 2) Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of the results.	• For AS-5.1.1: • SA-3 • • For AS-5.1.2: • CP-1, RA-3, • SA-3 • • For AS-5.1.3: • CP-1, CP-2, • SA-3
• AS-5.2: Take steps to prevent and minimize potential damage and interruption.	• AS-5.2.1: Backup files of key application data are created on a prescribed basis.	1) Review written policies and procedures for backing up and storing application data and programs.	• CP-9, SA-5
	• AS-5.2.2: Current application programs are copied and available for use	1) Examine the backup storage site.	• CP-6
	• AS-5.2.3: Backup files of application data and programs are securely stored offsite and retrievable for contingency plan implementation	1) Interview program and information technology officials and determine their assessment of the adequacy of backup policy and procedures.	• CP-6, CP-9
• AS-5.3: Develop and document an application Contingency Plan.	• AS-5.3.1: Develop a time-based application Contingency Plan.	1) Review the application contingency plan and broader scoped related plans.	• CP-2
	• AS-5.3.2: Incorporate the application Contingency Plan into related plans, such as the Disaster Recovery, Business Continuity, and Business Resumption Plans.	1) Determine whether the broader-scoped plans have incorporated the application contingency plan. 2) Compare the plan with guidance provided in NIST SP 800-34. 3) Interview program, information technology, and security administration officials and determine their input and assessment of the reasonableness of the plan.	• CP-2

	• AS-5.3.3: Contingency operations provide for an effective control environment by restricting and monitoring user access to application data and programs, including: • Users are identified and authenticated. • Users are properly authorized before being able to perform sensitive transactions. • Audit and monitoring capabilities are operating	1) Interview program, information technology, and security administration officials. Determine their assessment for providing an effective control environment during contingency operations. 2) Review the contingency plan and any test results for control related issues.	• CP-2, CP-4
• AS-5.4: Periodically test the application contingency plan and adjust it as appropriate.	• AS-5.4.1: The application contingency plan is periodically tested and test conditions include disaster simulations.	1) Review policies on testing. Determine when and how often contingency plans are tested.	• CP-4
	• AS-5.4.2: The following areas are included in the contingency test: • System recovery on an alternate platform from backup media • Coordination among recovery teams • Internal and external connectivity • System performance using alternate equipment • Restoration of normal operations • Notification procedures	1) Determine if technology is appropriately considered in periodic tests of the contingency plan and resultant adjustments to the plan. 2) Review test results. 3) Observe a disaster recovery test.	• CP-4
	• AS-5.4.3: Test results are documented and a report, such as a lessons-learned report, is developed and provided to senior management.	1) Review the final test report. 2) Interview senior management to determine whether they are aware of the test results.	• CP-4
	• AS-5.4.4: The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	1) Review any documentation supporting contingency plan adjustments.	• CP-5
• **Business Process Controls (BP)**			
• BP-1: Transaction data input is complete, accurate, valid, and confidential.			
• BP-1.1: A transaction data strategy is properly defined,	• BP-1.1.1: Data management procedures exist that include transaction data strategy, data design, data definitions, data quality standards, ownership and monitoring	1) Inquire of management and inspect documented policies and procedures related to data strategy. Inspect transaction data	• SA-3, SA-5

documented, and appropriate.	procedures. Data strategy should be unique to each data type.	strategy.	
• BP-1.2: Source documentation and input file data collection and input preparation and entry is effectively controlled.	• BP-1.2.1: Procedures are established to provide reasonable assurance that all inputs into the application have been authorized, accepted for processing, and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. Such procedures may include one or more of the following:- batch totals- sequence checking- reconciliations- control totals	1) Through inquiry, observation, and inspection, obtain an understanding of policies and procedures related to source document and input file collection and preparation, and determine whether the procedures are documented and properly designed. 2) Observe and inspect input preparation policies and procedures and relevant controls, noting procedures taken when exceptions are identified. 3) Inspect a selection of reports (a sample is not required, but the auditor could elect to choose one) used by management to determine whether the necessary inputs are accepted for processing, and inquire of review procedures used. 4) Inquire as to how source documents and input files are tracked and maintained and inspect relevant documentation.	• SI-1, SI-10, • SI-11
• BP-1.3: Access to data input is adequately controlled.	• BP-1.3.1: Procedures are implemented to control access to application input routines and physical input media (blank and completed).	1) Review procedures over control of data input to determine whether they are adequate. Coordinate this step with AS-2.	• SI-9
• BP-1.4: Input data are approved.	• BP-1.4.1: Documented approval procedures exist to validate input data before entering the system. Approval procedures are followed for data input.	1) Inspect documented procedures for approval of input data. 2) Inspect a selection of source documents (a sample is not required, but auditor could elect to choose one) and input files and determine whether the source data were approved for input.	• SI-1

• BP-1.5: Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.	• BP-1.5.1: Appropriate edits are used to reasonably assure that data are valid and recorded in the proper format, including: • authorization or approval codes; • field format controls; • required field controls; • limit and reasonableness controls; • valid combination of related data field values; • range checks • mathematical accuracy • master file matching • duplicate processing controls; and • balancing controls.	1) Through inquiry, observation, and inspection, understand edits used to reasonably assure that input data is accurate, valid, and in the proper format prior to being accepted by the application. The edits and procedures should address both manual and automated input processes. 2) Identify the key data input screens. Consider such factors as known errors and the frequency of use. If available, use analytical reports to support reasoning for screen selection. For the key manual input layouts identified, perform the following steps as applicable: • Observe an authorized data entry clerk inputting transactions, noting edits and validations for the various transaction entries. • Observe key transaction fields to determine whether they have adequate edit/validation controls over data input. • Obtain screen prints of appropriate scenarios and document the result. 3) For key automated inputs, observe and inspect data validation processes, completion controls, and exception reports in place. Inquire of management regarding procedures used to reject and resubmit data for processing, and procedures to provide reasonable assurance that data is not processed multiple times. 4) Note: to obtain evidence that the control was operating effectively, procedures would need to be applied at other points during the year.	• SI-10

	• BP-1.5.2: Edit and validation overrides are restricted to authorized personnel. Procedures exist to monitor, in a timely manner, overrides applied to transactions.	1) Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determining whether adequate review and follow up of overrides is performed. 2) Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).	• SI-9, SI-10
	• BP-1.5.3: Table maintenance procedures include edit and validation controls to help assure that only valid changes are made to data tables.	1) Through inquiry, observation, and inspection, obtain an understanding of table maintenance procedures relative to data edits and validation. 2) Observe an authorized person attempting to make invalid changes to tables, and confirm edits and validations are performed on changes.	• SI-10
• BP-1.6: Input values to data fields that do not fall within the tolerances or parameters determined by the management result in an input warning or error.	• BP-1.6.1: Parameters and tolerances are configured and error conditions and messages are defined. (These restrictions can be configured based on limits on transaction amounts or based on the nature of transactions) If a workflow is used so that documents can be released only by personnel with appropriate approval authority, then these requirements should be appropriately designed in the system. Management regularly reviews the restrictions placed on data input and validates that they are accurate and appropriate.	1) Inspect configuration of parameters and tolerance levels defined by the entity to identify whether the application accepts the data with warning or rejects the data, if the conditions are not met. 2) Inspect management review procedures, if the application accepts user data, with a warning. 3) Inspect the workflow rules and validate that the releasing authority is at an appropriate level. 4) Inspect evidence of management's regular review of relevant tolerances and parameters, and any correctional activities taken.	• SI-10, SI-11

• BP-1.7: Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected.	• BP-1.7.1: Procedures are established to reasonably assure that all inputs into the application have been accepted for processing and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. The procedures specifically require the exceptions to be resolved within a specific time period.	1) Inspect documented procedures related to data entry error handling procedures. 2) Inquire of management to determine which key management reports are used to monitor input errors. 3) Select a sample of input error reports and inspect to note evidence of management review. As applicable, inspect subsequent data input reports to note where data was corrected and resubmitted for processing.	• SI-11
• BP-1.8: Errors are investigated and resubmitted for processing promptly and accurately.	• BP-1.8.1: Data input errors are identified in suspense or error reports and resolved or resubmitted in a timely manner (within the period specified in the procedures).	1) Inspect a sample of recent suspense or error reports (can use sample selected in BP-1.7.1 provided information included will satisfy audit objectives for both audit procedures) and note whether suspense items are being corrected in a timely manner. Inspect the open items and note management's reasons for not correcting them in a timely manner.	• SI-1
• BP-2: Transaction data processing is complete, accurate, valid, and confidential.			
• BP-2.1: Application functionality is designed to process input data, with minimal manual intervention.	• BP-2.1.1: Application processing of input data is automated and standardized. Design documentation supporting the processing design exists for validation and change control purposes. The version of application, data and files to be processed are appropriate and current.	1) Inspect configuration and/or design documentation noting automatic and manual processing of transaction and information flow. Verify that proper versions of application, data and file are used.	• CM-3, SA-5, • SA-10
• BP-2.2: Processing errors are identified, logged and resolved.	• BP-2.2.1: System entries use transaction logs to reasonably assure that all transactions are properly processed and identify the transactions that were not completely processed.	1) Inspect a selection of application, transaction and error logs, noting whether all transactions were properly processed and missing or duplicate transactions were identified, including reruns and restarts.	• SI-10, SI-11

	• BP-2.2.2: Procedures are in place to identify and review the incomplete execution of transactions, analyze and take appropriate action.	1) Inspect selected incomplete transactions and validate that management has adequately investigated and corrected the errors or omissions. 2) Conduct a test with controlled group of live data and analyze the results with the expected values. Follow up with any exceptions.	• SI-1
	• BP-2.2.3: Procedures exist to monitor, in a timely manner, overrides applied to transaction processing.	1) Observe and inspect existing procedures for reviewer overrides or bypassing data processing routines. If an override log exists, observe and inspect to determining whether adequate review and follow up of overrides is performed. 2) Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).	• SI-1
• BP-2.3: Transactions are executed in accordance with the pre-determined parameters and tolerances, specific to entity's risk management.	• BP-2.3.1: Document processing and posting conditions (parameters and tolerances) are configured, including system errors and actions, if the are conditions are not met.	1) Inspect configuration of parameters and tolerances levels defined by the entity to identify whether the application processes the data with warning or rejects the data, if the conditions are not met.	• SI-10
	• BP-2.3.2: Management regularly reviews the restrictions to validate the accuracy and appropriateness.	1) Inspect management review procedures, noting management action when the application processes data or rejects it. In both cases, management should clearly analyze the impact on the downstream transactions.	• SI-1

• BP-2.4: Transactions are valid and are unique (not duplicated).	• BP-2.4.1: The application performs on-line edit and validation checks against data being processed. • BP-2.4.2: The system produces warning or error messages. • BP-2.4.3: Transactions with errors are rejected or suspended from processing until the error is corrected. • BP-2.4.4: The application communicates the processing error to the Users either on-line (if on-line entry) or via an exception report.	• Perform the following procedures for BP-2.4.1 to BP-2.4.4. 1) Inspect design document to identify key data validation and edit checks. 2) Inspect configuration to verify that the identified edit and validations checks are appropriately set, and transactions are rejected/suspended when data/processing errors occur. Also verify that warning and error messages are designed when the processing is incomplete. 3) Inspect the error communication methodology and assess 4) whether all processing errors are communicated to the users.	• For BP-2.4.1: • SI-10 • • For BP-2.4.2: • SI-11 • • For BP-2.4.3: • SI-11 • • For BP-2.4.4: • SI-11
• BP-2.5: The transactions appropriately authorized.	• BP-2.5.1: Transactions are matched with management's general or specific authorizations.	1) Review the adequacy of controls over authorization of transactions.	• SI-1
• BP-2.6: Data from subsidiary ledgers are in balance with the general ledger (step applicable to financial-related audits only).	• BP-2.6.1: Periodic reconciliation is performed and exceptions are appropriately handled.	1) Inspect periodic procedures to determine whether reconciliations are performed and documented with evidence. 2) For a selection of reconciliations, examine supporting evidence for adequacy. 3) Through inquiry, observations, and inspection, determine if the system is configured to auto balance, where possible.	• SI-1, SI-11
• BP-2.7: User-defined processing is adequately controlled.	• BP-2.7.1: Appropriate policies and procedures over user-defined processing are implemented. • BP-2.7.2: Controls over user-defined processing are adequate.	1) Review policies and procedures over user-defined processing. 1) Assess the operating effectiveness of user-defined processing.	• SA-5, SI-1 • SA-5, SI-1

• BP-2.8: As appropriate, the confidentiality of transaction data during processing is adequately controlled.	• BP-2.8.1: Management implements adequate controls to protect the confidentiality of data during processing, as appropriate.	1) Assess the adequacy of management controls over confidentiality during processing. 2) Coordinate this step with Critical Element AS-2 Implement effective application access controls.	• AC-3, AC-4, • SA-3, SA-5, • SA-8, SC-9, • SI-9, SI-10, • SI-11, SI-12
• BP-2.9: An adequate audit and monitoring capability is implemented.	• BP-2.9.1: Management has procedures in place to reconcile the data input with the data processed by the application.	1) Inspect procedures regarding reconciliation of transactions.	• SI-1
	• BP-2.9.2: Monitoring procedures should provide details of data to be added / modified during the processing, and expected result. System audit logs should be reviewed for exception.	1) Inspect operations activity at selected times and check for evidence that reconciliations are being performed.	• SI-1
	• BP-2.9.3: Management maintains a process log and the log is reviewed for unusual or unauthorized activity.	1) Inspect the processing log and note whether the unusual or unauthorized activity was followed up properly and promptly.	• SI-1
	• BP-2.9.4 Procedures exist to monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	1) Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. 2) If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.	• SI-1
• BP-3: Transaction data output is complete, accurate, valid, and confidential.			
• BP-3.1: Outputs are appropriately defined by the management. (form, sensitivity of data, user selectivity, confidentiality, etc.)	• BP-3.1.1: Management has developed a reporting strategy that includes the following: • content and availability that are consistent with end users' needs, • sensitivity and confidentiality of data • appropriate user access to output data.	1) Inquire of management about a reporting strategy or policy. Obtain a copy of any formal reporting strategy or policy. 2) Assess the adequacy of the strategy and related policies.	• SA-3, SA-5, • SI-1
• BP-3.2: Output generation and distribution are aligned with the reporting strategy.	• BP-3.2.1: Management has procedures in place to reasonably assure that content and availability of output and data are consistent with end users' needs, sensitivity, laws and regulations, and confidentiality of data and	1) Inspect management procedures for defining and assigning output/reports. 2) Select key output/reports in the area of audit scope and verify the user access to the	• AC-2, MP-2

	valid user access. • BP-3.2.2: Management has procedures in place to monitor replication of output data used in management reports or other communications within or outside the entity. • BP-3.2.3: User access to output data is aligned with the user's role and confidentiality/sensitivity of information.	output/reports. 1) Inquire of management on the use of data output. Inspect selected management reports or other communication to verify the accurate replication of data. 2) Verify that the user received appropriate authorization to use the data. 1) Review user access to selected output data and assess the appropriateness of access.	• SI-12 • SI-12
• BP-3.3: System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.	• BP-3.3.1: Management has identified key reports to track processing results. • BP-3.3.2: Management has documented procedures to review processed results, where applicable. • BP-3.3.3: Procedures are in place to review critical output data or control reports on a timely basis.	• Perform the following procedures for BP-3.3.1 to BP-3.3.3. 1) Inquire of user management and personnel to determine the key reports used to track processing results. 2) Obtain and inspect reports identified by management in the above test to determine whether the reports exist and are reviewed on a timely basis. 3) Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. 4) If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.	• For BP-3.3.1: • SI-1, SI-9, • SI-10, SI-11 • • For BP-3.3.1: • SI-1, SI-12 • • For BP-3.3.1: • SI-12
• BP-3.4: Output/ reports are in compliance with applicable laws and regulations.	• BP-3.4.1: Output reports for compliance with applicable laws and regulations are accurate, complete.	1) Inspect a sample of output/reports for compliance with applicable laws and regulations. 2) Identify laws and regulations that are to be complied with and verify that the reports are in compliance.	• SI-12
• BP-3.5: Access to output/reports and output files is based on business need and is limited to authorized users.	• BP-3.5.1: Access to reports is restricted to those users with a legitimate business need for the information. • BP-3.5.2: Users should have appropriate authorization for accessing reports, including the appropriate level of security	1) Perform the following procedures for BP-3.5.1 to BP-3.5.2. 2) Select output/reports and output files from the audit area and inspect application access (if the output can be accessed on-line or other electronic form) or inspect distribution to	• SI-12

	clearance, where applicable.	determine whether the user has appropriate level of security clearance and is authorized to access.	
• BP-4: Master data setup and maintenance is adequately controlled.			
• BP-4.1: Master data are appropriately designed.	• BP-4.1.1: An entry is required in all key fields, such as address and account number.	1) Inspect master data configuration for required field values.	• SA-3, SA-5
	• BP-4.1.2: Null values or invalid values are not accepted in the required fields.	1) Observe user input of invalid values, or blank values, and note any exceptions.	• SA-8
	• BP-4.1.3: For financial applications, account assignments (asset, liability, income and expense) are accurately defined.	1) Inspect master data configuration for account groups and assignments.	• SI-10
• BP-4.2: Changes to master data configuration are appropriately controlled.	• BP-4.2.1: Policies and procedures are established for master data configuration management, which include change rules that identify data fields that are excluded from changes (for example, master data number).	1) Review the master data polices and procedures for change management.	• SI-1
	• BP-4.2.2: Changes to the master data design are approved by appropriate personnel	1) Inspect a sample of change requests and verify that appropriate approvals are obtained. 2) Inspect master data configuration for change rules, if the rules are configured. If the change rules are automatic, then the user should be prevented from making unauthorized configuration changes.	• SA-10
	• BP-4.2.3: Changes to the master data records should be limited to non-key fields.	1) Inspect a sample of master data change reports and verify that changes are limited to management-defined non-key fields.	• SI-1, SI-10
• BP-4.3: Only valid master records exist.	• BP-4.3.1: Master data is reviewed on a regular basis, duplicates are identified and removed or blocked, and unused data is identified and blocked.	1) Inquire of management regarding their master data review procedures. 2) Inspect policies and procedures on master data review, including duplicate master data entry and resolution, and unused master records. 3) Inspect evidence of the most recent management review and action. 4) Inspect list of accounts/records blocked for	• SI-1

		posting or use. 5) Inspect duplicate master record report and management's use of it.	
	• BP-4.3.2: Automatic application controls (duplicate checks, system warnings) are configured to prevent and/or identify potential duplicate master records.	1) Inspect application configuration for automatic controls and determine whether the controls prevent erroneous processing or simply warn of potential errors.	• SI-10, SI-11
• BP-4.4: Master data are complete and valid.	• BP-4.4.1: Policies and procedures for master data maintenance are documented and include: • approval requirements; • data quality criteria; • data owner; • supporting documents; • backup procedures in the event of a disaster or data corruption error; • Archival policies.	1) Inspect master data maintenance policies and procedures for appropriateness. 2) Inquire of responsible personnel.	• SA-3, SI-1
	• BP-4.4.2: The master data maintenance process includes a formal create/change request from the requestor and approval from the data owner.	1) Select a sample of master data created or changed, and inspect relevant documentation, noting appropriate approvals and compliance with policies and procedures. 2) Obtain system report of users with master data maintenance access. For a sample of users with conflicting responsibilities, inspect user profiles noting evidence of segregation of duty consideration and review when conflicts are noted.	• SA-10, SI-9
	• BP-4.4.3: Segregation of duties conflicts are considered and resolved before providing access to master data transactions.	1) Inspect procedures for identifying, segregation of duty exceptions, and review compliance.	• AC-5, SA-5
	• BP-4.4.4: Edit reports are reviewed by appropriate data owners on a periodic basis to review new master data and changes made to existing master data.	1) Inspect evidence of proper review of edit reports by owners	• SI-10

• BP-4.5: Master data are consistent among modules.	• BP-4.5.1: Periodic review and reconciliation procedures are in place to ensure that master data are consistent between different application modules.	1) Inspect evidence of management reconciliation and review for effectiveness. 2) Through inquiry and inspection, determine whether the frequency of management reconciliation of master data is appropriate.	• SI-11
• BP-4.6: Master data additions, deletions, and changes are properly managed and monitored by data owners.	• BP-4.6.1: Master data policies and procedures require data owner's to be responsible for the creation, deletion, and change of master data and also changes to data characteristics.	1) Review policies and procedures and inquire of data owner concerning application of specific monitoring procedures.	• SA-3, SA-5, • SI-1
	• BP-4.6.2: Data owners monitor master data design changes, and approve and monitor creation, deletion and changes to master data on a regular basis.	1) Obtain and inspect evidence of monitoring by data owners, including related reports. 2) Inquire of management regarding ongoing monitoring of master data changes. 3) Obtain and inspect evidence of management review of master data design changes, and determine whether changes are approved and reviewed.	• SI-10, SI-11
• BP-4.7: As appropriate, the confidentiality of master data is adequately controlled.	• BP-4.7.1: Management implements adequate controls to protect the confidentiality of master data, as appropriate.	1) Assess the adequacy of management controls over confidentiality of master data. 2) Coordinate this step with Critical Element AS-2 Implement effective application access controls.	• AC-3, AC-4, • SA-3, SA-5, • SA-8, SC-9
• **Interface Controls (IN)**			
• IN-1: Implement an effective interface strategy and design.			
• IN-1.1: An interface strategy is developed for each interface used in the application.	• IN-1.1.1: An interface strategy exists for each interface that includes the interface method, data fields being interfaced, controls to reasonably ensure a complete and accurate interface, schedule, assignment of responsibilities, system balancing requirements and security requirements.	1) Obtain a list of all interfaces to and from the application audited. 2) Inspect the interface strategy document noting the details of each interface and determine whether it contains appropriate information.	• SA-3, SA-5
• IN-1.2: An interface design is developed for each interface	• IN-1.2.1: An interface design exists for each interface and includes appropriate specifications based on the business	1) Inspect interface design documents of each interface and determine whether it contains appropriate information.	• SA-3, SA-5

used in the application that includes appropriate detailed specifications.	requirements, including: • validations and edits • ownership of the interface process • error correction and communication methods		
	• IN-1.2.2: Mapping tables are used to convert data from the source system to the target system. Controls are in place to reasonably assure that mapping tables are only changed when authorized and that historical data on mappings is retained with the previous mapping table.	1) Determine whether the interfaces use mapping tables. Verify that controls over mapping tables will be established.	• SA-3, SA-5
	• IN-1.2.3: If mapping tables are not used, appropriate edits and validations are present in the source system.	1) Verify whether the appropriate edits and validations are implemented in the source systems.	• SI-9, SI-10, • SI-11
• IN-2: Implement effective interface processing procedures.			
• IN-2.1: Procedures are in place to reasonably assure that the interfaces are processed accurately, completely and timely.	• IN-2.1.1: Procedures include a complete list of interfaces to be run, the timing of the interface processing, how it is processed and how it is reconciled. If system interconnections are used, procedures should address requirements for an Interconnection Security Agreement and Memorandum of Understanding. Timing for processing of the interface has been determined and is followed. A positive acknowledgement scheme is used to ensure that files sent from a source system are received by the target system (i.e., a "handshake" between the systems so that files are not skipped or lost).	1) Inspect documentation of interface processing procedures and, if applicable, Interconnection Service Agreements and Memorandums of Understanding. 2) Observe interface processing into the application. 3) Determine whether data and files from interface activities are processed according to the stated policies and in the proper accounting period. 4) Determine whether all files sent from the source system are received and acknowledged by the target system.	• SA-5, SI-9, • SI-10, SI-11
• IN-2.2: Ownership for interface processing is appropriately assigned.	• IN-2.2.1: Responsibility for processing the interface and correcting any errors has been assigned to a user from the source and to a user of the target system. Actual processing may involve a technical person, if the interface is processed via an electronic media, such as a tape.	1) Identify which users are assigned responsibility for the interfaces. Evaluate whether an appropriate level of resources has been assigned to maintain interfaces.	• SA-2

	• IN-2.2.2: The files generated by an application interface (both source and target) are properly secured from unauthorized access and/or modifications.	1) Assess whether appropriate security is in place for all access points to the interface data are secure from unauthorized use. 2) Identify individuals that will be responsible for providing security surrounding the interfaces.	• AC-3
	• IN-2.2.3: Users who are processing interfaces are able to monitor the status of interfaces.	1) Assess whether proper access is assigned to the appropriate individuals for the monitoring of the interface status and that such individuals have access to appropriate information to monitor the status of the interface.	• AC-3
• IN-2.3: The interfaced data is reconciled between the source and target application to ensure that the data transfer is complete and accurate.	• IN-2.3.1: Reconciliations are performed between source and target applications to ensure that the interface is complete and accurate. Control totals agree between the source and target systems. Reports reconcile data interfaced between the two systems and provide adequate information to reconcile each transaction processed.	1) Inspect reports or other documents used to reconcile interface processing between source and target applications and review their content and frequency for appropriateness.	• SI-10
• IN-2.4: Errors during interface processing are identified by balancing processes and promptly investigated, corrected and resubmitted for processing.	• IN-2.4.1: Management maintains a log for interface processing. The log accounts for errors and exceptions, as well. Exception/error reports are produced, reviewed, and resolved by management on a regular basis, including correction and resubmission, as appropriate.	1) Through inquiry of management and review of logs, determine whether errors are properly handled. Assess the appropriateness of the frequency that exception reports are reviewed (daily, weekly, etc). Inspect evidence of such reviews having been performed.	• SI-10
• IN-2.5: Rejected interface data is isolated, analyzed and corrected in a timely manner.	• IN-2.5.1: Error and correction facilities are utilized to track and correct errors in interface data.	1) Assess the adequacy of procedures in place to properly correct any rejected transactions. 2) Inquire about procedures applied with individuals responsible for identifying and correcting errors and inspect evidence that rejected data is properly processed timely basis.	• SI-11
	• IN-2.5.2: A mechanism is used to notify	1) Determine whether error messages are	• SI-11

	users when data is rejected (for example, an e-mail message may be sent to the user). These messages should repeat daily until they are corrected.	generated and promptly reviewed for all rejected data and are maintained until corrected.	
	• IN-2.5.3: Audit trails are used to identify and follow-up on interface errors. The corrections to interface errors are included in the audit trail.	1) Determine whether appropriate audit trails are generated, reviewed and maintained.	• SI-10
• IN-2.6: Data files are not processed more than once.	• IN-2.6.1: Interfaces files are automatically archived or deleted from the production environment after processing.	1) Inspect a sample of archived interface documents and verify the date and time of processing. 2) Observe the interfaces that are in process and inspect evidence that they were not processed before in the same period.	• SI-10
• **Data Management System Controls (DA)**			
• DA-1: Implement an effective data management system strategy and design.			
• DA-1.1: Implement an effective data management system strategy and design, consistent with the control requirements of the application and data. The strategy addresses key concepts including: • database management, • middleware, • cryptography, • data warehouse, and • data reporting / data extraction.	• DA-1.1.1: The physical and logical (in terms of connectivity) location of the data storage and retrieval functions are appropriate.	1) Inspect documentation of the design of the data management system(s) associated with the application.	• SA-5
	• DA-1.1.2: The production data management system is effectively separated from non-production systems (such as testing and development) and other production systems with lesser control requirements.	1) Assess whether the production and nonproduction data management systems are effectively separated.	• SA-3, SA-5, • SA-10, SC-2
	• DA-1.1.3: The database schema is consistent with access control requirements such that the organization of data and database-hosted functions correspond to the access limitations that need to be imposed on different groups of users.	1) Verify that all access paths to data and sensitive data management system administrative functions have been identified and are adequately controlled.	• AC-3, SA-3, • SC-2
• DA-1.2: Detective controls are	• DA-1.2.1: Logging and monitoring controls are in place at the data management	1) Identify the security events that are logged and determine whether logging is adequate.	• AU-2, AU-3, • SA-5

implemented in a manner that effectively supports requirements to identify and react to specific system or user activity within the data management system and its related components.	system level which effectively satisfy requirements to accurately identify historical system activity and data access • DA-1.2.2: Real-time or near real-time controls are in place to detect abnormal activity and security events	2) Assess the adequacy of controls to monitor the audit logs. 1) Assess the adequacy of controls to detect abnormal activity.	• AU-5, AU-6, • SI-4, SI-5
• DA-1.3: Control of specialized data management processes used to facilitate interoperability between applications and/or functions not integrated into the applications (such as ad-hoc reporting) are consistent with control requirements for the application, data and other systems that may be affected.	• DA-1.3.1: Data accuracy and completeness controls are in place and effective to correct and/or detect data anomalies. • DA-1.3.2: The configuration of system connectivity that facilitates application to application and application to non-integrated functions is controlled to limit access appropriately.	• Perform the following procedures for DA-1.3.1 to DA-1.3.2 1) Identify and obtain an understanding of specialized data management processes used to facilitate interoperability. 2) Understand how system interconnectivity is controlled with respect to data management systems. 3) Assess the adequacy of controls over specialized management processes. These procedures should be closely coordinated with tests of general controls related to the data management systems. 4) Determine whether a periodic reconciliation process is implemented to ensure the data in a data warehouse matches the data from the source system.	• For DA-1.3.1 • SA-3, SA-5 • • For DA-1.3.2 • AC-4

APPENDIX III: DETAILED MMA 912 TESTING PROCEDURES

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

• Section II: Policies and Procedures to Reduce Risk	
• A. Read the policies and 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 RA. • 2. Review IT Security policies and procedures to ensure that they reduce the risk outlined in the RA. • 3. Ensure that IT Security policies and procedures are current.
• B. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	• 1. Review the most current SDLC. • 2. Review additional information (i.e., SSP) which outline security controls included in the cost of developing new systems • 3. Review software change control policies and procedures to ensure that changes are being controlled effectively.
• C. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	• 1. Perform inquiries of appropriate personnel regarding major systems maintained at the site. • 2. Review documentation indicating accreditations and certifications were performed for the noted systems. • 3. Ensure that accreditations and certifications are in compliance with FISMA policies .
• D. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.	• 1. Perform inquiries of appropriate personnel regarding systems for which controls have been tested. • 2. Review evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems. • 3. Review evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits. • 4. Ensure that all reviews have been performed within the scope of the review.
• E. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	• 1. Review the most recent CMS CSR. • 2. Gaps in compliance as documented in the CMSR. • 3. Review management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
• F. Determine if security policies and procedures include controls to address platform security configurations, and patch management.	• 1. Review platform security configuration policies and procedures. • 2. Review patch management policies and procedures.
• Section III: Review of System Security Plans	
• A. Determine if a security plan is documented and approved.	• 1. Review most current SSP. • 2. Review documentation indicating the SSP was approved by appropriate individuals.

• B. Determine if the plan is kept current.	• 1. Review previous and current SSP to ensure that updates have been made as necessary. • 2. Review the date of the most current SSP to ensure that it is in the scope of the review.
• C. Determine if a security management structure has been established.	• 1. Review the security management's organizational chart.
• D. Determine if IS responsibilities are clearly assigned.	• 1. Review the security management's organization chart. • 2. Review the security management's formal job descriptions.
• E. Determine if owners and users are aware of security policies.	• 1. Review security training schedules. • 2. Review security training materials. • 3. For a selection of owners and users ensure that they have attended the required trainings.
• F. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	• 1. Review the most current SDLC. • 2. Review additional SDLC policies and procedures to ensure that security polices and procedures have been incorporated. • 3. Perform inquiries of appropriate personnel regarding major systems maintained at the site • 4. Review documentation indicating accreditations and certifications were performed for the noted systems.
• G. Determine if hiring, transfer, termination and performance policies address security.	• 1. Review hiring policies and procedure to ensure that they address security. • 2. Review transfer policies and procedures to ensure that they address security. • 3. Review termination policies and procedures to ensure that they address security. • 4. Review performance policies and procedures (i.e., ROB and Performance Evaluations) to ensure they address security.
• H. Determine if employee background checks are performed.	• 1. Review policies and procedures for performing background checks. • 2. Select a sample of employees and ensure that background investigations have been completed.
• I. Determine if security employees have adequate security training and expertise.	• 1. Identify all employees responsible for administering security. • 2. Review training records and certifications for all security employees to ensure that adequate training has been received.
• J. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	• 1. Review policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures. • 2. Review documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.

• K. Determine if management ensures that corrective actions are effectively implemented.	• 1. Review policies and procedures for ensuring that corrective actions are effectively implemented. • 2. Review evidence that management ensures that corrective actions are effectively implemented.
• Section IV: Review of Security Awareness Training	
• A. Determine if employees have received a copy of the ROB.	• 1. Inquire of the appropriate personnel regarding the maintenance and distribution of the ROB for all types of employees. • 2. Review the most current version of the ROB. • 3. Select a sample of employees and ensure that they have received a copy of the most current version of the ROB.
• B. Determine if employee training and professional development has been documented and formally monitored.	• 1. Inquire of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development. • 2. Review policies and procedures regarding the documentation and formal monitoring of employee training and professional development. • 3. For a selected sample of employees, review evidence that training and professional development is documented and formally monitored.
• C. Determine if there is mandatory annual refresher training for security.	• 1. Review policies and procedures regarding mandatory annual refresher security training. • 2. Review the most recent security awareness training curriculum. • 3. For a selected sample of employees, review evidence that all attended the mandatory annual refresher security training.
• D. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.	• 1. Review policies and procedures regarding methods to make employees aware of security. • 2. Conduct a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas. • 3. Inspect evidence that methods to make employees aware of security are implemented.
• E. Determine if employees have received a copy of or have easy access to agency security 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 that they are the most current.
• F. Determine if security professionals have	• 1. Identify all employees responsible for administering security.

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.	• 2. Review training records and certifications for all security employees to ensure that adequate training has been received. • 3. Inquire of appropriate personnel regarding the documentation and tracking of application specific training for employees. • 4. Review the most recent application specific training curriculum. • 5. Inspect evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
• Section V: Review of periodic testing and evaluation of the effectiveness of IT security policies	
• A. Determine if management reports for the review and testing of IT security policies and procedures, including network RA, 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 RAs, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.
• B. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	• 1. Inspect evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
• C. Determine if remedial action is being taken for issues noted on audits.	• 1. Review policies and procedures for taking remedial action for issues noted on audits. • 2. Inspect evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.
• Section VI: Review of Remedial Activities, processes, and reporting for deficiencies	
• A. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	• 1. Review policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness. • 2. Inspect evidence that weaknesses are tracked in a formal database (or other manner). • 3. Inspect evidence that planned actions to address all IT security weaknesses is being tracked.
• B. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	• 1. Review policies and procedures for preparing the CAP. • 2. Review all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
• C. Determine the number and nature of security	• 1. Review policies and procedures for preparing CAPs.

IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	• 2. Review all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed. • 3. Inspect evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
• Section VII: Review of Incident Detection, reporting, and response	
• A. Determine that management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.	• 1. Review policies and procedures for monitoring systems and networks for unusual activity, and or intrusion attempts. • 2. Inspect evidence that management is monitoring systems and networks for unusual activity and/or intrusion attempts based on the policies and procedures.
• B. Determine if management has procedures to take and has taken action in response to unusual activity, intrusion attempts and actual intrusions.	• 1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur. • 2. Inspect evidence that management has taken action in response to unusual activity, intrusion attempts, and/or actual intrusions if any have occurred within the scope of the review.
• C. Determine that management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	• 1. Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur. • 2. Ensure that that policies and procedures are in accordance with FISMA standards.
• Section VIII: Policies and procedures for continuity of operations and related physical security safeguards for IT systems.	
• A. Determine if critical data and operations are formally identified and prioritized.	• 1. Review the Business Contingency Plan to ensure that critical data and operations are formally identified and prioritized.
• B. Determine if resources supporting critical operations are identified in contingency plans.	• 1. Review the Business Contingency Plan to ensure that resources supporting critical operations are identified.
• C. Determine if emergency processing priorities are established.	• 1. Review emergency processing priorities to ensure that they are formally documented.
• D. Determine if data and program backup procedures have been implemented.	• 1. Review data and program backup policies and procedures. • 2. Inspect evidence (i.e., backup logs) that data and program backup procedures have been implemented.
• E. Determine if adequate environmental controls have been implemented.	• 1. Inquire of data center manager concerning the environmental controls implemented in the data center. • 2. Perform Walkthrough of data center to ensure that adequate environmental controls have been implemented.
• F. Determine if staff have been trained to respond to emergencies.	• 1. Review emergency response policies and procedures. • 2. Review emergency response training curriculum.

	• 3. Inspect evidence that emergency response training has been provided for applicable staff.
• G. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	• 1. Ensure that hardware maintenance procedures exist to help prevent unexpected interruptions. • 2. Ensure that problem management procedures exist to help prevent unexpected interruptions. • 3. Ensure that change management procedures exist to help prevent unexpected interruptions.
• H. Determine if policies and procedures for disposal of data and equipment exist and include applicable Federal security and privacy requirements.	• 1. Review policies and procedures regarding the disposal of data and equipment to ensure that applicable Federal security and privacy requirements are included.
• I. Determine if an up-to-date contingency plan is documented.	• 1. Inspect evidence that the contingency plan was approved within the scope of the review.
• J. Determine if arrangements have been made for alternate data processing and telecommunications facilities.	• 1. Review the contingency plan to ensure that arrangements have been made for alternate data processing and telecommunications facilities. • 2. Review the contract with the organization that will provide alternate data processing and telecommunications operations if necessary.
• K. Determine if the plan is periodically tested.	• 1. Review policies and procedures regarding periodically testing the contingency plan. • 2. Inspect evidence that the contingency plan has been periodically tested.
• L. Determine if the results are analyzed and contingency plans adjusted accordingly.	• 1. Inspect evidence that the contingency plan is adjusted accordingly after the tests are performed and analyzed.
• M. Determine if physical security controls exist to protect IT resources.	• 1. Inquire of data center manager concerning the physical security controls implemented in the data center. • 2. Perform Walkthrough of data center to ensure that adequate physical security controls exist.

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. IS responsibilities are clearly assigned.	1. Reviewed the security plan. 2. Reviewed the security management's organization chart. 3. Reviewed the security management's formal job descriptions.
5. Owners and users are aware of security policies.	1. Reviewed documentation supporting or evaluating the awareness program. Observed a security briefing. 2. Interviewed data owners and system users. Determined what training they have received and if they are aware of their security-related responsibilities. 3. Reviewed memos, electronic mail files, or other policy distribution mechanisms. 4. Reviewed personnel files to test whether security awareness statements are current. 5. Called selected users, identified yourself as security or network staff, and attempted to talk them into revealing their password. 6. Reviewed security training schedules. 7. Reviewed security training materials. 8. For a selection of owners and users ensured that they have attended the required trainings.
6. Management periodically assesses the appropriateness of security policies and compliance with them.	1. Reviewed the reports resulting from recent assessments, including the most recent FMFIA report. 2. Determined when last independent review or audit occurred and reviewed results.

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

- 12. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.
  - 1. Identified all employees responsible for administering security.
  - 2. Reviewed training records and certifications for all security employees to ensure that adequate training has been received.
  - 3. Inquired of appropriate personnel regarding the documentation and tracking of application specific training for employees.
  - 4. Reviewed the most recent application specific training curriculum.
  - 5. Inspected evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.

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

- 1. Hiring, transfer, termination, and performance policies address security.
  - 1. Reviewed hiring policies and procedure to ensure that they address security.
  - 2. Reviewed transfer policies and procedures to ensure that they address security.
  - 3. Reviewed termination policies and procedures to ensure that they address security.
  - 4. Ensured that performance policies and procedures (i.e., ROB 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 ROB.	• 1. Inquired of the appropriate personnel regarding the maintenance and distribution of the ROB for all types of employees. • 2. Reviewed the most current version of the ROB. • 3. Selected a sample of employees and ensured that they have received a copy of the most current version of the ROB.
• 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 RAs. Discussed any discrepancies with appropriate officials.
• 3. Data sensitivity and integrity have been documented and data has been classified.	• 1. Reviewed evidence based on policies and procedures that data has been classified.
• A.4 Access to significant computerized applications (such as claims processing), accounting systems, and Medicare data is appropriately authorized, documented, and monitored, and includes approval by resource owners, procedures to control emergency and temporary access, and procedures to share and properly dispose of data.	
• 1. Resource owners have 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 that applicable Federal security and privacy requirements are included. • 2. Interviewed management and systems personnel regarding access restrictions. • 3. Observed personnel accessing systems software, such as sensitive utilities, and noted the controls encountered to gain access. • 4. Attempted to access the operating system and other systems software. • 5. Selected some systems programmers and determined whether management-approved documentation supports their access to systems software. • 6. Selected some application programmers and determined whether they are not authorized access. • 7. Determined the last time the access capabilities of system programmers were reviewed.
• 6. Passwords, tokens, or other devices are used to identify and authenticate users.	• 1. Reviewed pertinent policies and procedures. • 2. Reviewed security software password parameters. • 3. Observed users keying in passwords. • 4. Attempted to log on without a valid password; make repeated attempts to guess passwords. • 5. Assessed procedures for generating and communicating passwords to users. • 6. Reviewed a system-generated list of current passwords.

	• 7. Searched password file using audit software. • 8. Attempted to log on using common vendor supplied passwords. • 9. Interviewed users and security managers. • 10. Reviewed a list of IDs and passwords. • 11. Repeatedly attempted to log on using invalid passwords. • 12. Reviewed security logs. • 13. Reviewed pertinent policies and procedures. • 14. Reviewed documentation of such comparisons. • 15. Interviewed security managers. • 16. Made comparison using audit software. • 17. Viewed dump of password files (e.g., hexadecimal printout). • 18. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor obtained the assistance of a specialist.
• 7. Identification of access paths.	• 1. Reviewed access path diagram.
• 8. Logical controls over data files and software programs.	• 1. Interviewed security administrators and system users. • 2. Reviewed security software parameters. • 3. Observed terminals in use. • 4. Reviewed a system-generated list of inactive logon IDs, and determined why access for these users has not been terminated. • 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 systems software components and determined whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
  - 4. Performed an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.
  - 5. Obtained a list of all systems software on test and production libraries used by the entity.
  - 6. Verified that access control software restricts access to systems software.
  - 7. Using security software reports, determined who has access to systems software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they shall 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 that adequate physical security controls exist. • 3. Reviewed lists of individuals authorized access to sensitive areas and determined the appropriateness for access. • 4. Before becoming recognized as the auditor, attempted to access sensitive areas without escort or identification badges. • 5. Observed entries to and exits from facilities during and after normal business hours. • 6. Observed utilities access paths. • 7. Inquired of data center manager concerning the physical security controls implemented in the data center. • 8. Observed entries to and exits from sensitive areas during and after normal business hours. • 9. Reviewed procedures for the removal and return of storage media from and to the library.

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

and approved.	• 2. For a selection of emergency changes recorded in the emergency change log, reviewed related documentation and approval.
• 3. Systems software changes are authorized, tested, and approved before implementation.	• 1. Reviewed pertinent policies and procedures. • 2. Interviewed management and systems personnel. • 3. Reviewed procedures for identifying and documenting systems software problems. • 4. Interviewed management and systems programmers. • 5. Reviewed the causes and frequency of any recurring systems software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems. • 6. Determined what authorizations and documentation are required prior to initiating systems software changes. • 7. Selected recent systems software changes and determined whether the authorization was obtained and the change is supported by a change request document. • 8. Determined the procedures used to test and approve systems software prior to its implementation. • 9. Selected recent systems software changes were tested to verify indicated procedures were in fact used. • 10. Reviewed procedures used to control and approve emergency changes. • 11. Selected some emergency changes to systems software and tested whether the indicated procedures were in fact used.
• 4. Installation of systems software is documented and reviewed.	• 1. Interviewed management and systems programmers about scheduling and giving advance notices when systems software is installed. • 2. Reviewed recent installations and determine whether scheduling and advance notification did occur. • 3. Determined whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations. • 4. Interviewed management, systems programmers, and library control personnel, and determined who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries. • 5. Reviewed supporting documentation for some systems software migrations and the removal of outdated versions from production libraries. • 6. Interviewed data center management about their role in reviewing systems software installations. • 7. Reviewed some recent systems software installations and determined whether documentation shows that logging and management review occurred.

	• 8. Interviewed systems software personnel concerning a selection of systems software and determined the extent to which the operating version of the systems software is currently supported by the vendor. • 9. Interviewed management and systems programmers about the currency of systems software and the currency and completeness of software documentation. • 10. Reviewed documentation and tested whether recent changes are incorporated.
• 5. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	• 1. Reviewed the most current System Development Life Cycle. • 2. Reviewed additional information (i.e., SSP) which outline security controls included in the cost of developing new systems. • 3. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
• 6. Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	• 1. Performed inquiries of appropriate personnel regarding major systems maintained at the site. • 2. Reviewed documentation indicating accreditations and certifications were performed for the noted systems. • 3. Ensured that accreditations and certifications are in compliance with FISMA policies .
• A.8 A System Development Life Cycle methodology is documented and in use and includes planning for and costs for security requirements in systems.	
• 1. A SDLC has been implemented.	• 1. Reviewed SDLC methodology. • 2. Reviewed system documentation to verify that SDLC methodology was followed. • 3. Interviewed staff. • 4. Reviewed training records.
• 2. Management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	• 1. Reviewed additional information (i.e., SSP) which outline security controls included in the cost of developing new systems. • 2. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
• 3. Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	• 1. Reviewed additional System Development Life Cycle policies and procedures to ensure that security polices and procedures have been incorporated. • 2. Performed inquiries of appropriate personnel regarding major systems maintained at the site. • 3. Reviewed documentation indicating accreditations and certifications were performed for the noted systems
• A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.	

• 1. Authorizations for software modifications are documented and maintained.	• 1. Identified recent software modifications and determined whether change request forms were used. • 2. Examined a selection of software change request forms for approvals. • 3. Interviewed software development staff.
• 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; (7) reviewed test results; (8) reviewed documentation of management or security administrator reviews; (9) verified user acceptance; and (10) reviewed updated documentation. • 3. Determined whether operational systems experienced a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
• 4. Emergency processing priorities are established.	• 1. Reviewed emergency processing priorities to ensure that they are formally documented.
• 5. Data and program backup procedures have been implemented.	• 1. Reviewed data and program backup policies and procedures. • 2. Inspected evidence (i.e., backup logs) that data and program backup procedures have been implemented.
• 6. Hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.	• 1. Reviewed hardware maintenance procedures that exist to help prevent unexpected interruptions. • 2. Reviewed problem management procedures that exist to help prevent unexpected interruptions. • 3. Reviewed change management procedures that exist to help prevent unexpected interruptions.
• A.10 Access to program libraries is properly restricted and movement of programs among libraries is controlled.	
• 1. Programs are labeled and inventoried.	• 1. Reviewed pertinent policies and procedures. • 2. Interviewed personnel responsible for library control. • 3. Examined a selection of programs maintained in the library and assessed compliance with prescribed procedures. • 4. Determined how many prior versions of software modules are maintained.
• 2. Access to program libraries is restricted.	• 1. Examined libraries in use. • 2. Interviewed library control personnel.

	• 3. Verified that source code exists for a selection of production load modules. • 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 IPL 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	• 1. Reviewed pertinent policies and procedures.

implemented for using and monitoring use of system utilities.	• 2. Interviewed management and systems personnel regarding their responsibilities. • 3. Determined whether logging occurs and what information is logged. • 4. Reviewed logs. • 5. Using security software reports, determined who can access the logging files.
• 4. Inappropriate or unusual activity is investigated and appropriate actions taken.	• 1. Interviewed technical management regarding their reviews of privileged systems software and utilities usage. • 2. Reviewed documentation supporting their reviews. • 3. Interviewed management and systems personnel regarding these investigations. • 4. Reviewed documentation supporting these investigations. • 5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff. • 6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities. • 7. Interviewed management and analyzed their reviews concerning the use of systems software. • 8. Determined what management reviews have been conducted, and their currency, over this area.
• 5. Formal procedures guide personnel in performing their duties.	• 1. Reviewed manuals. • 2. Interviewed supervisors and personnel. • 3. Observed processing activities.
• 6. Active supervision and review are provided for all personnel.	• 1. Interviewed supervisors and personnel. • 2. Observed processing activities. • 3. Reviewed history log reports for signatures indicating supervisory review.
• A.13 A regular RA 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 RA policies. • 2. Reviewed the most recent high-level RA. • 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	• 1. Reviewed data classification policies and procedures

have been documented and if data have been classified.	• 2. Reviewed evidence based on policies and procedures that data have been classified
• 4. Threat sources, both natural and manmade, have been formally identified.	• 1. Reviewed RA to ensure that threat sources, both natural and man-made, have been identified and documented.
• 5. A list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.	• 1. Reviewed the RA to ensure that a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed. • 2. Reviewed the RA 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 RA to ensure that mitigating controls are documented. • 2. Reviewed the RA to ensure that mitigating controls have been assessed and documented to determine if they adequately mitigate vulnerabilities.
• 7. Final risk determinations and related management approvals have been documented and maintained on file.	• 1. Reviewed the RA to ensure that final risk determinations are documented. • 2. Reviewed RA and/or related documentation indicating it has been approved (currently).
• 8. A mission/business impact analysis have been conducted and documented.	• 1. Reviewed documented critical business processes. • 2. Reviewed mission/business impact analysis to ensure that it has been documented for the critical business processes.
• 9. Obtain management's list of additional controls that have been identified to mitigate identified risks.	• 1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
• 10. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.	• 1. Performed inquiries of appropriate personnel regarding systems for which controls have been tested. • 2. Reviewed evidence (i.e., internal/external audits) indicating system controls have been tested and evaluated for the identified systems. • 3. Reviewed evidence (i.e., internal/external penetration tests, etc) indicating system/network boundaries have been subjected to periodic reviews/audits. • 4. Ensured that all reviews have been performed within the scope of the review.
• A.14 A centralized risk management focal point for IT RA 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. IS responsibilities are clearly assigned.	• 1. Reviewed the security plan.
• 3. Final risk determinations and related	• 1. Reviewed the RA to ensure that final risk determinations are documented.

management approvals have been documented and maintained on file.	• 2. Reviewed RA and/or related documentation indicating it has been approved (currently).
• 4. Obtain management's list of additional controls that have been identified to mitigate identified risks.	• 1. Reviewed any additional documented lists of controls identified to mitigate identified risks.
• 5. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	• 1. Reviewed the most current RA. • 2. Reviewed IT Security policies and procedures to ensure that they reduce the risk outlined in the RA. • 3. Ensured that IT Security policies and procedures are current.
• 6. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	• 1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures. • 2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
• 7. Management reports for the review and testing of IT security policies and procedures, including network RA, 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 RAs, 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 RA and SSP has been documented, approved, and monitored by management in accordance with the CMS IS Risk Assessment and System Security Plan Procedures.	
• 1. Risks are periodically assessed.	• 1. Reviewed RA policies. • 2. Reviewed the most recent high-level RA. • 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 that corrective actions are effectively implemented.
- 2. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.
  - 1. Reviewed the most recent CMS CSR.
  - 2. Noted Gaps in compliance as documented in the CMSR.
  - 3. Reviewed management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
- 3. Weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.
  - 1. Reviewed policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness.
  - 2. Inspected evidence that weaknesses are tracked in a formal database (or other manner).
  - 3. Inspected evidence that planned actions to address all IT security weaknesses are being tracked.
- 4. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.
  - 1. Reviewed policies and procedures for preparing CAPs.
  - 2. Reviewed all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
- 5. The number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.
  - 1. Reviewed policies and procedures for preparing CAPs.
  - 2. Reviewed all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed.
  - 3. Inspected evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
- 6. Remedial action is being taken for issues noted on audits.
  - 1. Reviewed policies and procedures for taking remedial action for issues noted on audits.
  - 2. Inspected evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.
- A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.
- 1. An incident response capability has been implemented.
  - 1. Interview security manager, response team members, and system users.
  - 2. Review documentation supporting incident handling activities.
  - 3. Determine qualifications of response team members.

• 2. Audit trails are maintained.	• 1. Review security software settings to identify types of activity logged.
• A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts, and actual intrusions.	
• 1. Suspicious access activity is investigated and appropriate action is taken.	• 1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur. • 2. Tested a selection of security violations to verify that follow-up investigations were performed, and to determine what actions were taken against the perpetrator. • 3. Interviewed senior management and personnel responsible for summarizing violations. • 4. Reviewed any supporting documentation. • 5. Reviewed policies and procedures and interviewed appropriate personnel. • 6. Reviewed any supporting documentation.
• 2. Inappropriate or unusual activity is investigated and appropriate actions taken.	• 1. Interviewed technical management regarding their reviews of privileged systems software and utilities usage. • 2. Reviewed documentation supporting their reviews. • 3. Interviewed management and systems personnel regarding these investigations. • 4. Reviewed documentation supporting these investigations. • 5. Interviewed systems programmer supervisors to determine their activities related to supervising and monitoring their staff. • 6. Reviewed documentation supporting their supervising and monitoring of systems programmers' activities. • 7. Interviewed management and analyzed their reviews concerning the use of systems software. • 8. Determined what management reviews have been conducted, and their currency, over this area.
• A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the Federal Information Security Management Act (FISMA)	
• 1. Management processes and procedures include reporting of intrusion attempts and intrusions in accordance with FISMA guidance.	• 1. Reviewed polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur. • 2. Ensured that policies and procedures are in accordance with FISMA standards.