CMS Manual System

Pub. 100-17 Medicare Business Partners Systems Security

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal 4 **Date: MARCH 5, 2004**

CHANGE REQUEST 3106

I. SUMMARY OF CHANGES:
The sections and appendices of the Medicare Business Partners Systems Security Manual were updated to provide correct links to the CMS website and other reference documents, expand on security concepts, clarify core security requirements and security activities to be conducted/followed, include due dates for system security activities and make minor editorial changes.

NEW/REVISED MATERIAL - EFFECTIVE DATE: February 1, 2004
***IMPLEMENTATION DATE: April 5, 2004**

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

II. CHANGES IN MANUAL INSTRUCTIONS: (R = REVISED, N = NEW, D = DELETED

R/N/D	CHAPTER/SECTION/SUBSECTION/TITLE
R	1.0/Introduction
R	2.2/The (Principal) Systems Security Officer (SSO)
R	3.0/IT Systems Security Program Management
R	3.1/System Security Plan (SSP)
R	3.2/Risk Assessment
R	3.3/Certification
R	3.4/Information Technology Systems Contingency Plan
R	3.5.1/Annual Compliance Audit
R	3.5.2/Corrective Action Plan
R	3.6.1/Computer Security Incident Response
R	4.1/Information Security Levels
R	4.1.2.4/Level 4: High Criticality and National Security Interest
R	4.2/Sensitive Information Protection Requirements
R	4.2.1/Restricted Area
R	4.2.2/Security Room
R	4.2.3/Secured Interior/Secured Perimeter
R	4.2.4/Container

N	4.2.4.1/Locked Container
N	4.2.4.2/Security Container
N	4.2.4.3/Safe/Vaults
N	4.2.5/Locking Systems for Secured Areas and Security Rooms
N	4.2.6/Intrusion Detection Equipment (IDS)
R	5.0/Internet Security
R	Appendix A/Core Security Requirements and the Contractor Assessment Security Tool (CAST)
N	Attachment A/CMS Core Set of Security Requirements
R	Appendix B/Medicare Information Technology (IT) Systems Contingency Planning
R	Appendix C/An Approach to Fraud Control
R	Appendix E/Glossary

*III. FUNDING:

These instructions should be implemented within your current operating budget.

IV. ATTACHMENTS:

X	**Business Requirements**
X	**Manual Instruction**
	Confidential Requirements
	One-Time Notification
	Recurring Change Notification

***Medicare contractors only**

Attachment - Business Requirements

Pub. 100-17	Transmittal: 4	Date: March 5 2004	Change Request 3106

SUBJECT: Medicare Business Partners Systems Security (a.k.a. CMS Business Partners Systems Security Manual)

I. GENERAL INFORMATION

A. Background: This document provides Medicare Contractors with Federal laws and regulations for security compliance. It also gives the processes required to complete security activities and the associated due dates during the current fiscal year.

B. Policy: CMS is authorized by the Secretary of the Department of Health and Human Services to protect its information systems and all data and information that is processed, produced, stored and/or transmitted on the government's behalf.

C. Provider Education: None.

II. BUSINESS REQUIREMENTS

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

Requirement #	Requirements	Responsibility
3106	Medicare Contractors shall follow and implement all security activities and requirements as outlined in the Medicare Business Partners Systems Security Manual.	All Medicare Contractors

III. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions:

X-Ref Requirement #	Instructions
N/A	N/A

B. Design Considerations:

X-Ref Requirement #	Recommendation for Medicare System Requirements
N/A	N/A

C. Interfaces: None.

D. Contractor Financial Reporting /Workload Impact: None.

E. Dependencies: None.

F. Testing Considerations: None.

IV. SCHEDULE, CONTACTS, AND FUNDING

Effective Date: February 1, 2004 **Implementation Date: April 5, 2004** **Pre-Implementation Contact(s): Sherwin Schulterbrandt** **Post-Implementation Contact(s): same as above.**	**These instructions shall be implemented within your current operating budget**

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

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

CMS/Business Partners

Systems Security Manual

(Rev. 4, 03-05-04)

Appendices

1.0 Introduction

(Rev. 4, 03-05-04)

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

A CMS business partner is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, fiscal intermediaries, Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.

This manual addresses the following key business partner security elements:

- An overview of primary roles and responsibilities.
- A program management planning table that will assist System Security Officers (SSOs) and other security staff in coordinating a system security program at a business partner site.
- Appendix A: CMS Core Security Requirements (CSRs) and the Contractor Security Assessment Tool (CAST), which provides the following:
    - An overview of the Core Security Requirements; and
    - An overview of the Contractor Assessment Security Tool (CAST).

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

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

  http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm
- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996.

- Public Law 106-398, National Defense Authorization Fiscal Year 2001, Government Information Security Reform Act (GISRA) of 2000.
- Office of Management and Budget (OMB) Circular No. A-127, Financial Management Systems, June 21, 1995.
  http://www.whitehouse.gov/omb/circulars/index.html
- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999.
  http://www.whitehouse.gov/omb/circulars/index.html
- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000.
  http://www.whitehouse.gov/omb/circulars/index.html
- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000.
  http://www.whitehouse.gov/omb/circulars/index.html
- Presidential Decision Directive/NSC – 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998.
  http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
- GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999.
  http://www.gao.gov/special.pubs/ai12.19.6.pdf
- CMS System Security Plans (SSP) Methodology, Draft Version 3.0, October 28, 2002.
  www.cms.hhs.gov/it/security
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, June 2000.
  http://www.irs.gov/pub/irs-pdf/p1075.pdf

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

- Department of Health and Human Services, Automated Information Systems Security Program Handbook (DHHS AISSP).
  http://wwwoirm.nih.gov/policy/aissp.html
- NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC), November 1991.
  http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, SP800-12.
  http://csrc.nist.gov/publications/nistpubs/800-12
- Code of Federal Regulations, Regulation 36 CFR Part 1228 Subpart K, NARA36
  http://www.access.gpo.gov/nara/cfr/cfrhtml_00/Title_36/36cfr1228_00.html
- Code of Federal Regulations, Regulation 5 CFR Part 731 – Suitability, 5CFR731
  http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html

- FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25 U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, PUB 46-3.

  http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- CMS Internet Security Policy

  www.cms.hhs.gov/it/security
- *CMS Information Security Risk Assessment (RA) Methodology, Version # 1.1September 12, 2002.*

  http://www.cms.hhs.gov/it/security/

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

2.2 The (Principal) Systems Security Officer (SSO)

(Rev. 4, 03-05-04)

Business partners must designate a Systems Security Officer (SSO) qualified to manage the Medicare system security program and assure the implementation of necessary safeguards.

The SSO must be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development. A qualified SSO that is available to direct security operations full time provides the foundation for the security culture and awareness of the organization. A sound entity-wide security program is the cornerstone to ensure implementation and maintenance of effective security controls. The SSO position in each contractor should be a full-time position staffed with an individual fully qualified, and preferably credentialed, in systems security. Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available Line One funding.

A business partner may have additional SSOs at various organizational levels, but they must coordinate security actions through the principal SSO for Medicare records and operations. The SSO assures compliance with CMS Core Security Requirements by performing the following:

- Facilitating the Medicare IT system security program and assuring necessary safeguards are in place and working.
- Coordinating system security activities throughout the organization.
- Ensuring that IT systems security requirements are considered during budget development and execution.
- Reviewing compliance of all components with the CMS Core Security Requirements and reporting vulnerabilities to management.

- Establishing an incident response capability, investigating systems security breaches, and reporting significant problems (see Section 3.6) to business partner management, and CMS.
- Ensuring that technical and operational security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes.
- Ensuring that IT systems security requirements are included in RFPs and subcontracts involving the handling, processing, and analyzing of Medicare data.
- Maintaining systems security documentation in the Systems Security Profile for review by CMS and external auditors.
- Cooperating in all official external evaluations of the business partner's systems security program.
- Facilitating the completion of the Risk Assessment (see Section 3.2).
- Ensuring that an operational Information Technology Systems Contingency Plan is in place and tested (see Section 3.4).
- Documenting and updating the Corrective Action Plans (see Section 3.5). Updates follow issuance of new requirements, risk assessment, internal audit, external evaluation, and, of course, the target dates themselves. (The schedule and updates are highly sensitive and should have limited distribution.)
- Keeping all elements of the business partner's System Security Profile secure (see Section 3.7).
- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix B).

The Principal Systems Security Officer should earn 40 hours of continuing professional education credits from a recognized national information systems security organization each year.

3.0 IT Systems Security Program Management

(Rev. 4, 03-05-04)

Business partners must implement policies, procedures, controls, or plans that fulfill the CMS Core Security Requirements (see Appendix A).

Understand that meeting requirements does not validate the quality of the program. Managers with oversight responsibility must understand the processes and methodology behind the requirements. The following Table 3.1 identifies key requirements and provides high-level descriptions of them. As appropriate, this section refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners must perform a self-assessment using the CMS Core Security Requirements. The supporting documentation, planned safeguards, and related schedules must be recorded using the Contractor Assessment Security Tool (CAST), (see Appendix A, Section A-2). To perform the self-assessment, business partners must conduct a systematic review of the Core Security Requirements using CAST. CAST provides a self-assessment form that includes audit protocols to assist in the review of the requirements.

The CMS Core Security Requirements include key security-related tasks. *Table 3.1* indicates when or how often these tasks need to be rechecked, the disposition of output or documentation, comments, and a space to indicate completion or a "do by" date. The number accompanying each entry in the requirement column indicates the section of this document that deals with the particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule.

Table 3.1. Planning Table

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
Appendix A, Section 2, Self-Assessment using CAST	Each Federal fiscal year.	CCMO/PO with a copy to CMS CO. Systems Security Profile	See Appendix A, Section 2, for an overview of CAST. Self-assessment results recorded using CAST are to be discussed within the Certification Package.	□

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.1 System Security Plans	Each Federal fiscal year for each GSS and MA, or upon significant change.	Systems Security Profile. SSO CMS CO	System Security Plans are to be reviewed and updated as necessary and are to be discussed within the Certification Package. More information about System Security Planning can be found in the CMS SSP Methodology.	□
3.2 Risk Assessment (Report)	Every year or upon significant change.	Systems Security Profile *CMS CO*	*Risk Assessments are to be discussed within the Certification Package. The Risk Assessment Report is an attachment of the System Security Plan.* More information about Risk Assessment Reports can be found in the CMS Information Security RA Methodology.	□
3.3 Certification	Each Federal fiscal year.	CCMO/PO with a copy to CMS CO.	*Each year CMS will publish in Chapter 7 (internal controls) of its Financial Management Manual (Pub 100-6) information on certification requirements including where, when, and to whom these certifications must be submitted.*	□

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.4 Information Technology Systems Contingency Plan	Each Federal fiscal year, or upon significant change. Plans must be tested annually.	Systems Security Profile *SSO* CMS CO	Management and the SSO must approve the Plan. Plans are to be discussed within the Certification Package and should be conducted in accordance with Appendix B, Medicare IT Systems Contingency Planning. More information about contingency planning can be found in An Introduction to Computer Security: The NIST Handbook. Special Pub 800-12, and Contingency Planning Guide for Information Technology Systems: NIST Special Pub 800-34.	□

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.5 Compliance	Each Federal Fiscal year.	*CCMO/PO* *Systems Security Profile* *SSO* *CMS CO* *May be stored as paper documents, electronic documents, or a combination.*	There are two (2) components to compliance: (1) Annual Compliance **Audit:** Once a year, an independent audit will be performed on four (4) categories of the CMS Core Security Requirements to validate the self-assessment. CMS will determine the four categories the audit will validate by way of a Program Memorandum (PM). **(2) Corrective Action Plan** Corrective Action Plans address findings of annual systems security assessments including the Annual Compliance Audit, annual core security requirements review, SAS 70 audits (if any), and *CFO* controls audits (if any). CAST (see Appendix A, Section 2) will record all items assessed as “Partial” or “Planned.” The Corrective Action Plan addresses all “Partial” and “Planned” items, along with their “Comments/Explanations” and “Projected Completion Dates.”	□ □

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.6 Incident Reporting and Response	As necessary.	CCMO/PO Systems Security Profile	The HIPAA also addresses Incident Reporting information.	□
3.7 System Security Profile	As necessary.	On file in the Security Organization.		□

LEGEND:

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

When submitting documentation to CCMOs or CMS Central Office, use Federal Express, certified mail, or the equivalent (receipt required). Contact addresses are as follows:

- CMS CO

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

The following are the contacts and addresses of the four Consortia:

- Northeast Consortium

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

- Southern Consortium

  Consortium Contractor Management Officer
  Atlanta Regional Office
  Atlanta Federal Center, 4th Floor
  61 Forsyth Street, SW, Suite 4T20
  Atlanta, GA 30303-8909
  404-562-7250

- Midwest Consortium

  Consortium Contractor Management Officer
  Chicago Regional Office
  233 N. Michigan Avenue, Suite 600
  Chicago IL 60601
  312-353-9840

- Western Consortium

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

3.1 System Security Plan (SSP)

(Rev. 4, 03-05-04)

The objective of an Information Security (IS) program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process or store Medicare-related data have some level of sensitivity and require protection. The protection of a system must be documented in an SSP. The completion of an SSP is a requirement of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, Computer Security Act of 1987. All Medicare claims-related applications and systems must be covered by SSPs if they are categorized as a Major Application (MA)[1] or General Support System (GSS)[2].

The purpose of the SSP is to provide an overview of the security requirements of the system and describe the controls that are implemented to meet those requirements. The SSP also delineates

[1] Major Application–An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A major application can be either a major software application or a combination of hardware/software. Its sole purpose is to support a specific business-related function.

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

responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager (i.e., SSO).

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

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

All business partner Medicare claims-related SSPs must be developed in accordance with the most current version of the CMS System Security Plans (SSP) Methodology which is available on the CMS web site at: http://www.cms.hhs.gov/it/security. Business partners must also use the most current version of the Microsoft® Word© SSP template which is also available at the same web site.

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

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

A newly developed or updated SSP including the ORIGINAL signed and dated CMS SSP certification form (Tab A, Appendix A of the CMS SSP Template) must be sent to the CMS Central Office (Security and Standards Group; Mail Stop N2-14-26; 7500 Security Blvd.; Baltimore, MD 21244-1850). These documents must be received by CMS ten (10) working days after they have been developed, updated, or recertified. These documents must be submitted in hard copy and on CD-ROM. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

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

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

3.2 Risk Assessment

(Rev. 4, 03-05-04)

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

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

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

All RAs must be recertified within 365 days from the last date certified. Medicare Contractors must review their RA(s) prior to recertification to determine if an update is needed. An RA must be performed if a significant change[3] *to any information system has occurred. Examples of*

[3] The National Institute of Standards and Technology defines "significant change to an information systems is any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of

significant change include but are not limited to transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review and/or the updated RA must be placed in the Medicare Contractor's System Security Profile. The updated RA(s) must also be mailed to the CMS Central Office. The RA used to support a SSP(s) cannot be dated more than 12 months earlier than the SSP certification date.

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

A newly developed or updated RA which is an attachment to the SSP must be sent to the CMS Central Office (Security and Standards Group; Mail Stop N2-14-26; 7500 Security Blvd.; Baltimore, MD 21244-1850). These documents must be received by CMS ten (10) working days after they have been developed, updated, or recertified. These documents must be submitted in hard copy and on CD-ROM. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

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

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

Business Partners should refer to the Acceptable Risk Safeguards document to aid in the preparation of a risk assessment. This document can be found at www.cms.hhs.gov/it/security.

3.3 Certification

(Rev. 4, 03-05-04)

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

Each contractor is required to self-certify to CMS its IT systems security compliance within each Federal fiscal year. This security certification will be included in the *Certification Package for Internal Controls (CPIC).* CMS will continue to require annual, formal re-certification within

the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."

each fiscal year no later than September 30, including validation at all levels of security as described in this manual.

Systems Security certification must be fully documented and maintained in official records. The Certification validates that the following items have been developed and are available for review in the System Security Profile:

- Certification,
- Self-assessment (see Appendix A),
- System Security Plan for each GSS and MA (see Section 3.1),
- Risk Assessment (see Section 3.2 and CMS Information Security RA Methodology),
- Information Technology Systems Contingency Plan (see Section 3.4 and Appendix B),
- Results of Annual Compliance Audit (see Section 3.5), and
- Corrective Action Plans (see Section 3.5).

Each year CMS will *publish in Chapter 7 (internal controls) of its Financial Management Manual (Pub 100-6)* information on certification requirements including where, when, and to whom these certifications must be submitted.

3.4 Information Technology Systems Contingency Plan

(Rev. 4, 03-05-04)

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

- Reviewed whenever new systems are planned or new safeguards contemplated
- Reviewed annually to make sure they remain feasible
- Tested annually. If backup facility testing is done in segments, test each individual Medicare segment every year.

Appendix B to this manual provides information on Medicare Information Technology Systems Contingency Plans. See Item 3.4 in Table 3.1 of this manual for other references.

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

A newly developed or updated Medicare IT System Contingency Plan must be submitted to CMS within 10 working days after the business partner's management and SSO have approved it. A *hard copy and a copy on CD-ROM of the IT System Contingency Plan must be sent to the CMS Central Office. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.*

3.5.1 Annual Compliance Audit

(Rev. 4, 03-05-04)

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

CMS will notify business partners of which four categories will be included in the current year's audit. See Appendix A, Section A-2, for a description of the 10 categories of CMS Core Security Requirements.

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

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

The Annual Compliance Audit Report must include the following:

1. A Summary of Controls: These controls are those instructions that the business partner has implemented to comply with the CMS CSRs. The summary of controls should be derived from the source documentation referenced in the Contractor Assessment Security Tool (CAST).
2. A Description of Review Procedures and Tests: This description must include procedures and tests performed by the organization (internal or external) performing the Annual Compliance Audit as well as a description of the results of such tests.

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

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

The annual compliance audit (ACA) must be completed by September 30, 2004. The categories of the CMS Core Security Requirements (CSR) to be audited in fiscal year 2004 are: segregation of duties, service continuity, and networks. In lieu of auditing a fourth category of CSRs, the audit should review all incomplete FY 2002 funded safeguards (as of September 30, 2003) and FY 2003 funded safeguards (if any). The audit should assess: (1) the reasonableness of the safeguard to the CSR; (2) the reasonableness of the implementation cost (estimated or actual); (3) the reasonableness of the project plans to complete the safeguard; and (4) the effectiveness of the implementation of the safeguard.

Also, the ACA must assess the reasonableness and effectiveness of the Corrective Action Plans (CAPs) developed as a result of any CMS directed Statement on Audit Standards No. 70 (SAS 70) and/or Office of Inspector General Chief Financial Officer's Electronic Data Processing Control (OIG CFO EDP) audit finding(s). The ACA must include a recommendation of whether the CAP reasonably addresses the finding(s). Once addressed, the Medicare Contractor must make a formal recommendation to the CCMO/Consortium Contractor Management Staff (CCMS) to verify that the CAP has been satisfied.

A copy of the completed ACA must be submitted in hard copy and on CD-ROM to the CMS Central Office, your CCMO for Title XVIII contracts or PO for FAR contracts by October 14, 2004. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used. A copy must also be placed in the Systems Security Profile.

CMS recommends the ACA report be organized by subject matter to facilitate the ease of review and use. The categories should include (1) CAST CSR Categories, (2) Funded FY02 and FY04 (if any) Safeguards, (3) OIG CFO EDP audit, (4) SAS 70 review, and (5) any miscellaneous issues not covered by the above categories.

3.5.2 Corrective Action Plan

(Rev. 4, 03-05-04)

The second component of compliance requires the preparation of a CAP. Medicare business partners must review their security compliance and determine the degree of compliance to the CMS Core Security Requirements. *Section 3.5 of the BPSSM, like Chapter 7, Section 40 of Pub 100-6, requires the timely preparation and submission of Corrective Action Plans (CAPs). All CAP submissions must have target completion dates that realistically reflect when the information technology (IT) findings will be resolved. The milestone dates and action information must be listed in the contractor's CAP reports. Milestone data must be estimated and projected correctly to avoid data variances, and must be reported in the contractor's CAP report. CAPs must be prepared within ten (10) working days after the completion of the Annual Compliance Audit for any noted deficiencies.* It includes a status of scheduled implementation actions to assure that approved safeguards are in place or in process. When an item in the plan is a major risk, feedback will be provided by CMS within ninety (90) days of submission.

The Corrective Action Plan shall contain milestone dates, such as:

- Date a particular safeguard can be ordered/initiated
- Dates of various stages of implementation

CAST (see Appendix A, Section A-2) will record all items assessed as "Partial" or "Planned*.*" The Corrective Action Plan *addresses the* "Partial" and "Planned" items, along with their "Comments/Explanations" and "Projected Completion Dates*.*"

A copy of the completed CAP must be submitted in hard copy and on CD-ROM to the CMS Central Office, your CCMO for Title XVIII contracts or PO for FAR contracts by October 14, 2004. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used. A copy must also be placed in the Systems Security Profile.

Business partners are strongly encouraged to develop a project plan for all CAPs that cannot be resolved within 30 calendar days. A project plan enables the owner and other interested parties (i.e. CMS and auditors) to track its progress and ensure they are on schedule as planned. Project plans provide more detail than the general information contained in a CAP. The project plan should document the safeguard, (major) milestone dates, and the necessary steps or actions taken to resolve the CAP. These steps may include activities, responsible entities, and cost (if any). Supporting documentation, such as invoices, should be included as attachments to the project plan. The project plan should be maintained in the systems security profile and made available for review.

3.6.1 Computer Security Incident Response

(Rev. 4, 03-05-04)

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

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

Business partners should also contact the CMS Service Desk (410-786-2580) and report any confirmed security incident. Business partners should report the date and time when events occurred or were discovered; names of systems, programs, or networks effected by the incident; and impact analysis. Release of information during incident handling must be on an as-needed/need-to-know basis. When other entities would be notified of incidents at external business partner sites, CMS would coordinate with legal and public affairs contacts at the effected entities.

Business Partners should refer to The CMS System Security Incident Handling Procedures for further guidance. This document can be found at www.cms.hhs.gov/it/security.

4.1 Information Security Levels

(Rev. 4, 03-05-04)

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

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

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

Table 4.1. Summary of Sensitivity and Criticality Levels

Level	Sensitivity	Criticality
1	Threats to this data are minimal and only minimal precautions to protect the data need to be taken. Unintentional alteration or destruction is the primary concern for this type of data.	Systems requiring minimal protection. In the event of alteration or failure, it would have a minimal impact or could be replaced with minimal staff time or expense. This includes data that has low or no sensitivity.
2	Data has importance to CMS and must be protected against such acts as malicious destruction. However, because this type of data is most often collected for analytical purposes, disclosure problems are not usually significant.	Systems that are important but not critical to the internal management of CMS. If systems fail to function for an extended period of time, it would not have a critical impact on the organizations they support. This includes data that has moderate sensitivity.
3	The most sensitive unclassified data processed within CMS IT systems. This data requires the greatest number and most stringent information security safeguards at the user level.	Systems that are critical to CMS. This includes systems whose failure to function for even a short period of time could have a severe impact or has a high potential for fraud, waste, or abuse. This includes data that has high sensitivity.

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

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

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

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

Business partner System Owners/Managers and System Maintainers/Developers must ensure that their databases and the processing capabilities of their systems are accessed only by authorized users who fully use the required security level safeguards. The business partner managers of compartmentalized systems must take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The security level designation determines the minimum-security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities.

4.1.2.4 Level 4: High Criticality and National Security Interest

(Rev. 4, 03-05-04)

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

4.2 Sensitive Information *Protection* Requirements

(Rev. 4, 03-05-04)

Business partners are responsible for implementing a Minimum Protection Standard (MPS) for all CMS Level-3 – High-Sensitivity (CMS sensitive) information and materials. The MPS applies to all IT facilities, areas, or systems processing or storing CMS sensitive information in any form or on any media. The following chart should be used to determine the minimum standards required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The following alternative methods are not listed in any order of preference or security significance.

Table 4.2. Protection Alternative Chart

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

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

The objective of these standards is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security: (1) secured perimeter/ locked container, (2) locked perimeter/ secured interior, or (3) locked perimeter/ security container. Locked means a perimeter, area, or container that has both a lock and keys or combinations that are controlled. A security container is a lockable metal container with a resistance to forced penetration, with both a security lock and keys or combinations that are controlled. (See the following sections for additional explanation and details on these requirements.)

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

4.2.1 Restricted Area

(Rev. 4, 03-05-04)

A restricted area is an area whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas must either meet secured area criteria ***or*** *provisions* *must be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information.*

Restricted areas will be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance must have controlled access (electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

4.2.2 Security Room

(Rev. 4, 03-05-04)

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

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

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

4.2.3 Secured Interior/Secured Perimeter

(Rev. 4, 03-05-04)

Secured areas are internal areas that have been designed to prevent undetected entry by unauthorized persons during non-working hours. Secured areas/ secured perimeters must meet the following minimum standards:

- *Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, **or** any lesser-type partition (i.e., slab-to-slab walls) supplemented by UL-approved electronic IDS and fire detection systems.*
- *Unless electronic IDS devices are used, all doors entering the space must be locked, and strict key or combination control should be exercised.*

- *In the case of a fence and gate, the fence must have IDS devices* ***or*** *be continually guarded, and the gate must be either guarded or locked with intrusion alarms.*
- *The space must be cleaned during working hours in the presence of a regularly assigned employee.*

4.2.4 Container

(Rev. 4, 03-05-04)

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, and any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 Locked Container

(Rev. 4, 03-05-04)

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

4.2.4.2 Security Container

(Rev. 4, 03-05-04)

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

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

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

4.2.4.3 Safes/Vaults

(Rev. 4, 03-05-04)

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

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

4.2.5 Locking Systems for Secured Areas and Security Rooms

(Rev. 4, 03-05-04)

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

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

4.2.6 Intrusion Detection Equipment (IDS)

(Rev. 4, 03-05-04)

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

5.0 Internet Security

(Rev. 4, 03-05-04)

Use of the Internet is prohibited for health care transactions (claims, remittances, etc.) between Medicare carriers/ intermediaries and providers. This Internet prohibition also applies to the transport of CMS Privacy Act-protected data between carriers/ intermediaries and any other party. See the CMS Internet Security Policy for a definition of protected data at www.cms.hhs.gov/it/security, and Program Memoranda AB-01-11 (CR 1439) and AB-01-85 (CR 1749) for this Internet prohibition.

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

(Rev. 4, 03-05-04)

1.0 *CMS Core Security Requirements*

(Rev. 4, 03-05-04)

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

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

The CMS Core Security Requirements were developed by assessing requirement statements from a number of Federal and CMS mandates, including the following:

- Office of Management and Budget (OMB) Circular No. A-127, Financial Management Systems, June 21, 1995.

  http://www.whitehouse.gov/omb/circulars/index.html

- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999.

  http://www.whitehouse.gov/omb/circulars/index.html

- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000.

  http://www.whitehouse.gov/omb/circulars/index.html

- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000.

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

- Presidential Decision Directive/NSC – 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998.

  http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999.

  http://www.gao.gov/special.pubs/12_19_6.pdf

- CMS System Security Plans (SSP) Methodology Draft Version 3.0, October 28, 2002.

  www.cms.hhs.gov/it/security

- IRS 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, June 2000.

  http://www.irs.gov/pub/irs-pdf/p1075.pdf

- Health Insurance Portability and Accountability Act (HIPAA), 1996.

  http://aspe.os.dhhs.gov/admnsimp/pl104191.htm

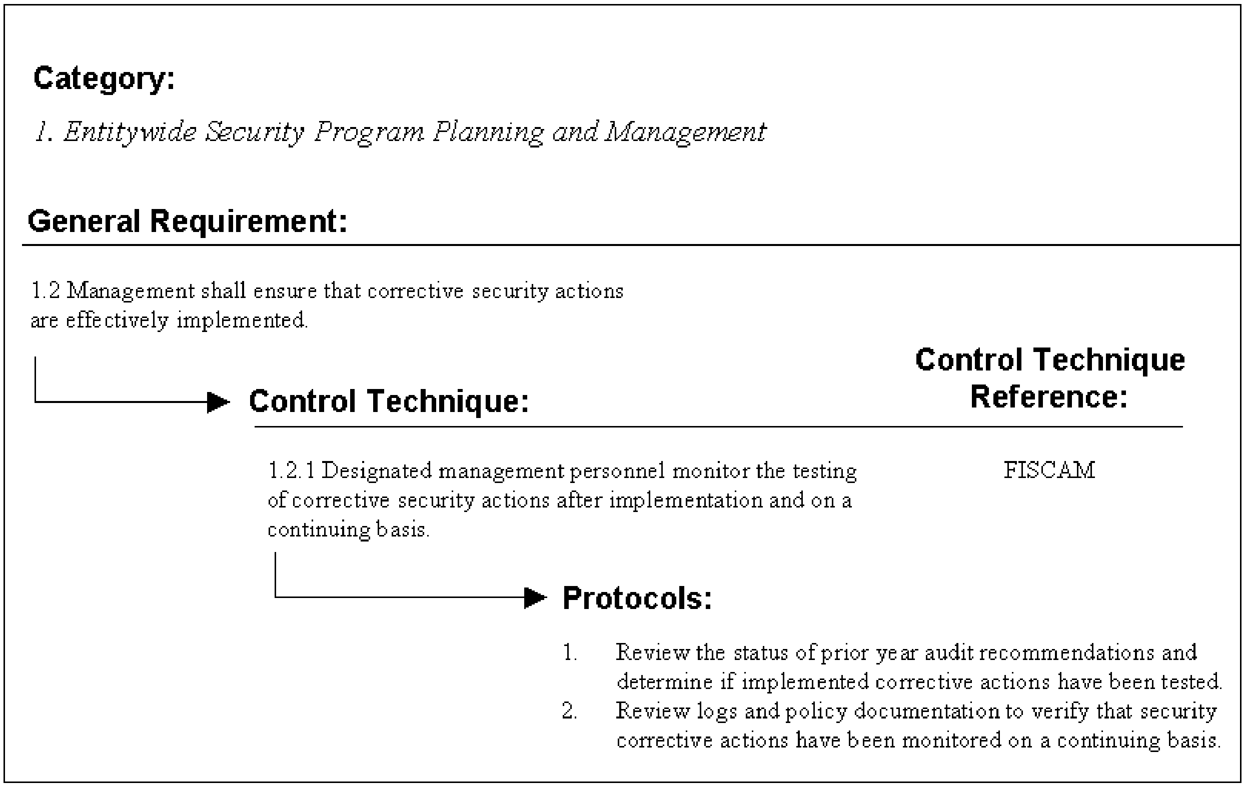
  http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm

CMS has organized the Core Security Requirements into Categories, General Requirements, Control Techniques, and Protocols. There are ten Categories comprised of six general Categories, three application Categories, and an additional Category, "Networks." The ten categories are as follows:

Category	Description
Entity-wide Security Program Planning and Management Elements	These controls address the planning and management of an entity's control structure.
Access Control	These controls provide reasonable assurance that information-handling resources are protected against unauthorized loss, modification, disclosure, *and* damage. *Access* controls *can be* logical *or* physical.
System Software	These controls address access and modification of system software. System software is vulnerable to unauthorized change and this category contains critical elements necessary for providing needed protection.
Segregation of Duties	These controls describe how work responsibilities should be

Category	Description
	segregated so that one person does not have access to or control over all of the critical stages of an information handling process.
Service Continuity	These controls address the means by which the entity attempts to ensure continuity of service. A business partner cannot lose its capability to process, handle, and protect the information it is entrusted with.
Application Software Development and Change Control	These controls address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information.
Application System Authorization Controls	These controls address the processing of Medicare data in a manner that ensures that only authorized transactions are entered into the information processing system.
Application System Completeness Controls	These controls ensure that all system transactions are processed and that any missing or duplicate transactions are identified and a remedy implemented.
Application System Accuracy Controls	These controls address the accuracy of all data entered into systems for processing, handing, and storage. Data must be valid and accurate. All invalid, erroneous, or inaccurate data must be identified and corrected.
Networks	These controls address the network structure. The network structure must be protected and the data transmitted on the networks must be protected.

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



Category:

1. Entitywide Security Program Planning and Management

General Requirement:

1.2 Management shall ensure that corrective security actions are effectively implemented.

Control Technique:

1.2.1 Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis.

Control Technique Reference:

FISCAM

Protocols:

1. Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested.
2. Review logs and policy documentation to verify that security corrective actions have been monitored on a continuing basis.

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

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

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

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

- Guidance - Additional guidance has been developed to clarify issues and provide additional information regarding each CSR. This information is available in the CAST during the self-assessment process, and may be printed from the forms menu.
- Related CSRs - Each CSR may be related to one or more other CSRs. It may be important that CSR responses be coordinated between these related CSRs. Business partners should take care to ensure that these related CSR responses are not conflicting. This information is available in the CAST during the self-assessment process, and may be printed from the forms menu.

- CSR Responsibility - A matrix has been developed jointly with CMS and business partner security experts to indicate where responsibility may lie for addressing the requirement of each CSR. This matrix indicates a best estimate of whether a particular CSR is applicable to a given contract type. While this matrix is not meant to be used as a requirements document, it does give business partners and CMS reviewers an indication of whether a particular CSR should be addressed by a given business partner. This information is available in the CAST during the self-assessment process, and may be included in output printed from the "Print Reports*."*

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

Because CMS Core Security Requirements and Protocols have retained their source references, business partners can conduct "modular" self-assessments that address the likely audit procedures that would be used by an external agency. For example, to prepare for an audit by the IRS, a business partner System Security Officer (SSO) could review the Core Requirements specifically associated with the IRS 1075. Additionally, by using the CAST tool (described in Section A-2 below), the SSO could use references in the CAST database to determine the location of a requirement in the IRS 1075. The SSO could also perform a preparatory self-assessment based only on those requirements that have the IRS 1075 as a source.

It should be noted that Control Techniques referenced as MCM/MIM (6/92) refer to information contained in the 6/92 version of the Medicare Carriers Manual and Medicare Intermediary Manual. Because the requirements are still relevant, they are incorporated into the Core Security Requirements.

See Appendix A for a copy of the CMS Core Security Requirements in Adobe Acrobat (.pdf) *format.*

2.0 The Contractor Assessment Security Tool (CAST)

(Rev. 4, 03-05-04)

2.1 Core Security Requirement Responses

(Rev. 4, 03-05-04)

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

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

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

The CMS will release CAST Version 4.0 to Medicare Contractors during FY2004. The CAST will be available for download from the CMS website. The Medicare Contractors must complete the CAST self assessment and submit a copy on CD-ROM to the CMS Central Office and the Consortia Contractor Management Officer (CCMO) for Title XVIII contracts or the Project Officer (PO) for FAR contracts by close of business April 30, 2004. A copy of the CAST self-assessment must be placed in the Systems Security Profile. Please be advised that this information should not be submitted to the CMS via email. Registered mail or its equivalent should be used. Should you need technical assistance, contact the CMS/NGIT Help Desk at (703)-620-8585.

2.1.1 All Responses

(Rev. 4, 03-05-04)

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

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

b) Each CSR requires a "Status" to be selected, and each CSR requires a detailed explanation in the CAST Explanation/Comment field to describe and explain the compliance status. In addition, all CSR responses must include a complete description of Who, What, Where, Why, and How each CSR is or is not in compliance, depending on the CSR status selection.

c) Where a merging of responsibilities occurs between business partners (such as the interface between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in *the Explanation/ Comments field. The description should include local responsibilities as well as those that are perceived to be responsibilities of some other CMS business partner.*

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

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

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

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

Business partners are required to enter a current status and comment or explanation for each CSR. The annual self-assessment is one of the central documents in the business partner's security profile and should reflect sufficient detail to convey to CMS the current status of the business partner's security program. In order to assist with the development of responses to the CSRs, the following decision tree has been developed to assist in the establishment of the current status of the business partner security.

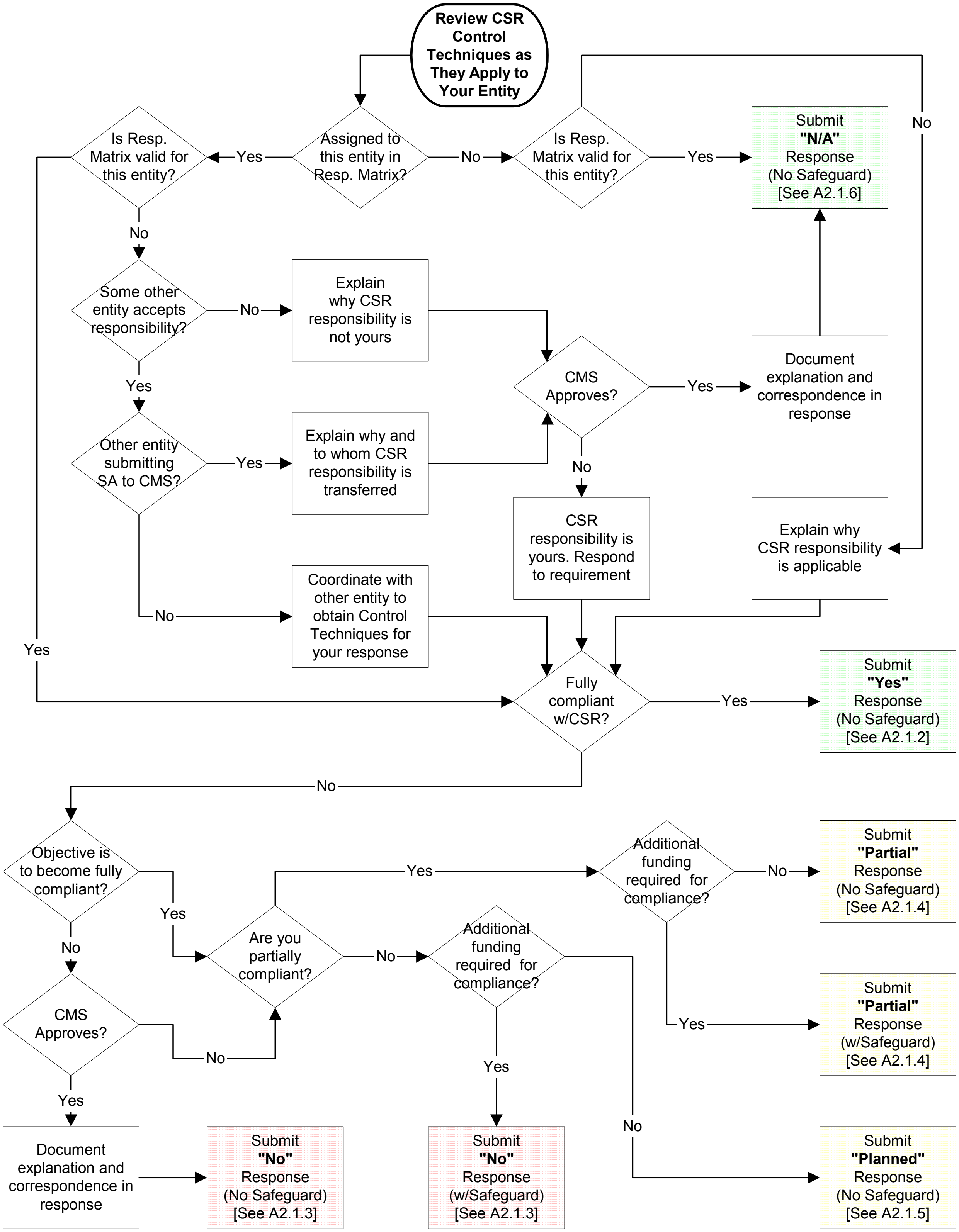

Review CSR Control Techniques as They Apply to Your Entity
Is Resp. Matrix valid for this entity?
Yes
Assigned to this entity in Resp. Matrix?
No
Is Resp. Matrix valid for this entity?
Yes
Submit "N/A" Response (No Safeguard) [See A2.1.6]
No
No
Some other entity accepts responsibility?
No
Explain why CSR responsibility is not yours
CMS Approves?
Yes
Document explanation and correspondence in response
Yes
Other entity submitting SA to CMS?
Yes
Explain why and to whom CSR responsibility is transferred
No
CSR responsibility is yours. Respond to requirement
Explain why CSR responsibility is applicable
No
Coordinate with other entity to obtain Control Techniques for your response
Yes
Fully compliant w/CSR?
Yes
Submit "Yes" Response (No Safeguard) [See A2.1.2]
No
Objective is to become fully compliant?
Yes
Yes
Additional funding required for compliance?
No
Submit "Partial" Response (No Safeguard) [See A2.1.4]
No
Are you partially compliant?
No
Additional funding required for compliance?
CMS Approves?
No
Yes
Submit "Partial" Response (w/Safeguard) [See A2.1.4]
Yes
Yes
No
Document explanation and correspondence in response
Submit "No" Response (No Safeguard) [See A2.1.3]
Submit "No" Response (w/Safeguard) [See A2.1.3]
Submit "Planned" Response (No Safeguard) [See A2.1.5]

Figure A-2. "Status" Decision Tree

2.1.2 Yes Responses

(Rev. 4, 03-05-04)

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

a) ***Who*** *is the principal point-of-contact (POC) for questions involving this requirement?*

The principal POC should be clearly delineated. This will ensure that detailed questions and requests for clarification can be addressed quickly and efficiently. While CMS will work directly with the SSO for resolution of issues, recording of the individual POC for each CSR will greatly simplify the SSO's resolution process.

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

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

c) ***Where*** *can applicable documentation be found?*

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

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

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

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

iii) In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.

e) Safeguards – The "Safeguard" button is disabled for a response with a status of "Yes."

No additional Safeguards or funding information can or should be provided. If additional Safeguards or funding are required to fully implement this response, the response status should be changed to either "Partial" or "No."

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

"Security Awareness Training is conducted during initial employee orientation and every year during the month of November for all employees and contractors. It includes all aspects outlined in the CSR Control Techniques as documented in company policy NG 7541-S3. The records of attendance are maintained in the Corporate Training Office, on the fifth floor of Bldg. #5 (cabinet #5). POC is Jim Socrates (401) 555-1212."

2.1.3 No Responses

(Rev. 4, 03-05-04)

A response status of "No" indicates that none of the Control Technique requirements are currently being met and there is no funded plan for meeting these requirements. If a funded plan does exist and has already been fully funded (i.e., no further funding allocation is required), the response status should be "Planned." If a plan exists but *requires additional funding that is not currently allocated or available for Safeguard implementation, then the response status should be "No" and a Safeguard generated with appropriate funding requirements indicated. If the business partner does not meet the requirements of the CSR and has no plans to implement a Safeguard that will fully meet the CSR Control Techniques, then the response status should be "No." In this case, written notification to CMS must be provided (and acknowledged by CMS) that the CSR at issue is not currently being addressed and the business partner does not intend to attempt to meet the applicable compliance requirements. The Explanation/ Comments field should, at a minimum, contain a detailed explanation of the Who, Why, and How. These minimum requirements are listed below:*

a) ***Who*** *is the principal POC for questions involving this requirement?*

   i) *The principal POC should be clearly delineated. This will ensure that detailed questions and requests for clarification can be addressed quickly and efficiently. While CMS will work directly with the SSO for resolution of issues, recording of the individual POC for each CSR will greatly simplify the SSO's resolution process.*

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

   i) *Funded vs. Unfunded plans:*

      (1) *A funded plan consists of a documented timetable and existing funding. Funding may consist of corporate funding, existing Line One funding, and/or some other previously awarded funding.*

         (a) *If a funded plan exists for implementation of a suitable control, but has not yet been implemented, then a detailed explanation must be provided outlining the obstacles to implementation of any funded Safeguards.*

      (2) *A plan is considered unfunded if it requires additional funding that is not currently allocated or available for Safeguard implementation. A Safeguard should be generated with appropriate funding requirements indicated.*

(a) If there is currently no funded plan for meeting compliance with this CSR, a detailed explanation must be provided outlining all of the obstacles to implementation of a suitable control (including Safeguards and funding requirements).

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

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

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

(1) Date CMS acknowledged the response,

(2) CMS office that acknowledged the response, and

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

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

d) Safeguards – The "Safeguard" button is enabled for a response with a status of "No." Safeguards should be developed to address the CSR. If funding is required to change systems, policies, or procedures in order to become compliant with this CSR, the Safeguards should describe (in detail) the funding requirements. Not all Safeguards require additional funding. Many Safeguards are already funded through existing funding sources and should therefore be answered with a status of "Planned." Details on how to develop Safeguards within the CAST are provided in a later section.

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

"Our file server system uses a Green Hat Linux 1.0 operating system. This version of Linux is hard-coded to display the password while entering. G. Iam Secure [(401) 555-1234] contacted (via phone) I. M. Programmer at Green Hat [(651) 555-4321] on 8/31/00 to determine if an update to correct this discrepancy is underway. Mr. Programmer indicated that the password will continue to be displayed through the next revision, but future changes are tentatively planned. Investigation into alternative software has resulted in no suitable software packages. CMS was informed in writing on 9/30/00 and CMS acknowledged in writing on 10/15/00. Applicable correspondences are maintained in file cabinet 8b on the third floor of the Operations Building."

2.1.4 Partial Responses

(Rev. 4, 03-05-04)

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

a) ***Who** is the principal POC for questions involving this requirement?*

   The principal POC should be clearly delineated. This will ensure that detailed questions and requests for clarification can be addressed quickly and efficiently. While CMS will work directly with the SSO for resolution of issues, recording of the individual POC for each CSR will greatly simplify the SSO's resolution process.

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

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

c) ***Where** can applicable documentation be found?*

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

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

   i) *Funded vs. Unfunded plans:*

      (1) *A funded plan consists of a documented timetable and existing funding. Funding may consist of corporate funding, existing Line One funding, and/or some other previously awarded funding.*

          If a funded plan exists for implementation of a suitable control, but has not yet been implemented, then a detailed explanation must be provided outlining the obstacles to implementation of any funded Safeguards.

      (2) *A plan is considered unfunded if it requires additional funding that is not currently allocated or available for Safeguard implementation. A Safeguard should be generated with appropriate funding requirements indicated.*

          If there is currently no funded plan for meeting compliance with this CSR, a detailed explanation must be provided outlining all of the obstacles to *implementation of a suitable control (including Safeguards and funding requirements).*

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

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

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

ii) *Describe in detail how the remaining Control Techniques will be brought into compliance by the Projected Completion Date.*

iii) *In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.*

f) *Enter a "Projected Completion Date":*

All "Partial" resolutions or controls require a "Projected Completion Date." A response with a status of "Partial" indicates that ongoing efforts to become fully compliant are underway. If no further efforts are underway or planned for becoming fully compliant, then the response status should be changed to "No."

g) *Safeguards – The "Safeguard" button is enabled for a response with a status of "Partial." Additional Safeguards may be developed to address the CSR, but are not necessarily required. If existing controls are in the process of being implemented, but are not fully in place, no new controls are required or generated. If additional controls are required to change systems, policies, or procedures in order to become compliant with this CSR, the newly developed Safeguards should be described in detail and the funding requirements specified. Not all Safeguards require additional funding. Many Safeguards are already funded through existing funding sources. Details on how to develop Safeguards within the CAST are provided in a later section.*

Example entry for a CSR with a response status of "Partial" and a Safeguard requiring additional funding:

"We use a mainframe and an off-site data storage facility connected via a T1 line and triple-DES encryption. However, the local corporate distributed network (WAN), which may process some administrative documents containing sensitive patient information, is connected via DSL and T1 lines to remote facilities without encryption. Additional network encryption devices are required for the local corporate distributed LAN. Documentation on our existing and planned encryption techniques is maintained in the Security Department, on the second floor of Bldg. #2 (cabinet #2). The POC in the

Security Department is Iam Secure (401) 555-1234.
Projected Completion Date: 2/10/2002"

Example entry for a CSR with a response status of "Partial" that is fully funded:

"We use a mainframe and an off-site data storage facility connected via a T1 line and triple-DES encryption. The local corporate distributed network (WAN), which may process some administrative documents containing sensitive patient information, is connected via DSL and T1 lines to remote facilities without encryption. CMS approved and funded the purchase and installation of the triple-DES encryption devices for the mainframe system as well as for network encryption devices for the local corporate distributed LAN. The mainframe encryption devices were installed on 11/14/02 but the LAN network encryption devices are currently on back order. Because the applicable Safeguard is already approved and funded, no additional funding is required for this CSR. Documentation on our existing and planned encryption techniques is maintained in the Security Department, on the second floor of Bldg. #2 (cabinet #2). The POC in the Security Department is Iam Secure (401) 555-1234.
Projected Completion Date: 2/10/2003"

2.1.5 Planned Responses

(Rev. 4, 03-05-04)

A response status of "Planned" indicates that while none of the Control Technique requirements are currently being met, a funded plan of action exists to remedy the situation. A funded plan consists of a documented timetable and existing funding. Funding may consist of corporate funding, existing Line One funding, and/or some other previously awarded funding. If a plan exists but requires additional funding that is not currently allocated or available for Safeguard implementation, then the response status should be changed to "No." Enter a "Projected Completion Date" (required) and describe how the system will be brought into compliance. The Explanation/ Comments field should, at a minimum, contain a detailed explanation of the Who, What, Where, Why, and How. These minimum requirements are listed below:

*a) **Who** is the principal POC for questions involving this requirement?*

The principal POC should be clearly delineated. This will ensure that detailed questions and requests for clarification can be addressed quickly and efficiently. While CMS will work directly with the SSO for resolution of issues, recording of the individual POC for each CSR will greatly simplify the SSO's resolution process.

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

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

*c) **Where** can the funded plan be found?*

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

d) ***Why** is this CSR not being met? What efforts are underway in an attempt to fully resolve this issue?*

   i) *Funded plans:*

   A funded plan consists of a documented timetable and existing funding. Funding may consist of corporate funding, existing Line One funding, and/or some other previously awarded funding.

   If a funded plan exists for implementation of a suitable control, but has not yet been implemented, then a detailed explanation must be provided outlining the obstacles to implementation of any funded Safeguards.

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

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

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

   ii) *In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.*

f) *Enter a "Projected Completion Date":*

   All "Planned" resolutions or controls require a projected completion date. "Planned" means that a documented timetable exists. If no completion date is available, then the response status should be changed from "Planned" to "No."

g) *No funding information can be provided for a response with a response status of "Planned." If additional funding is required to fully implement this response, the response status should be changed to either "Partial" or "No."*

h) *Safeguards – The "Safeguard" button is disabled for a response with a status of "Planned." No new Safeguards or funding requirements may be provided for a response with a status of "Planned." If additional funding or Safeguards are required to fully implement this response, the response status should be changed to either "Partial" or "No."*

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

"A training plan and training materials do not exist for new employee orientation training. New employee training is being developed in a joint effort between the Security Department

and the IT Training Department. The security training outline is complete and on file in the Corporate Training Office on the fifth floor of Bldg. #5 (cabinet #5). No additional Safeguards or funding is required to meet the requirements of this CSR. The training POC is Jim Socrates (401) 555-1212. The POC in the Security Department is Iam Secure (401) 555-1234
Projected Completion Date: 2/10/2002"

2.1.6 N/A Responses

(Rev. 4, 03-05-04)

A response status of "N/A" indicates that the Control Technique requirements are not applicable to this contract type. Except as indicated in the CAST CSR Gap Responsibilities matrix, most, if not all, CSRs are applicable to all portions of all business partner contracts. Where an intersection of responsibilities occurs between business partners (such as the interface between Data Centers and claims processors or between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in the Explanation/Comments field. When Control Technique requirements have been subcontracted out to a third-party contractor or are being performed for this contract entity by another corporate entity, the ultimate responsibility for implementing and reporting compliance (or non-compliance) remains with the primary contract holder, so the response must be some status other than "N/A." The Explanation/ Comments field should, at a minimum, contain a detailed explanation of the Who, Why, and How. These minimum requirements are listed below:

a) ***Who*** *is the principal POC for questions involving this requirement?*

   The principal POC should be clearly delineated. This will ensure that detailed questions and requests for clarification can be addressed quickly and efficiently. While CMS will work directly with the SSO for resolution of issues, recording of the individual POC for each CSR will greatly simplify the SSO's resolution process.

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

   A complete and detailed description should be provided to describe the circumstances that render the subject CSR "N/A" to a particular business partner. Referral to the applicability matrix is NOT sufficient justification for an "N/A" response. A full understanding of the reasons for non-applicability must be demonstrated in the CSR response.

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

   i) *CMS expects all CSRs to be addressed by all business partners. Very few CSRs are expected to receive occasional "N/A" responses based on answers provided in alternative CSRs (see example). Where a merging of responsibilities occurs between business partners (such as the interface between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in the Explanation/ Comments field (as it applies to this contract type). Note that even if data processing duties are subcontracted out to either another CMS business partner (such as a Data Center) or to some third-*

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

ii) Include the following information with CMS-approved "N/A" responses:

(1) Date CMS approved the response,

(2) CMS office that approved the response, and

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

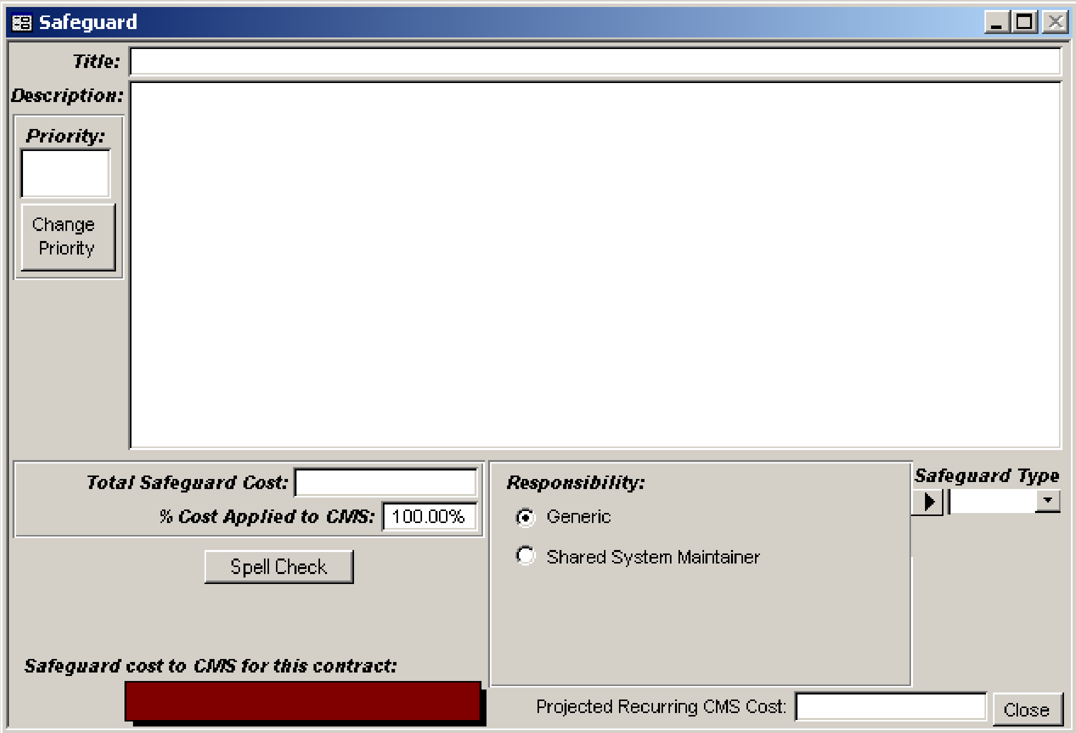
Example entry for a CSR with a response status of "N/A":

"This requirement describes the required features of "security rooms." CSR 2.2.25 suggests "security rooms" as one of several possible methods, but does not require one. We use "secured areas" and "appropriate containers" (CSR 2.2.19 and 2.2.5). This issue was discussed via letter to CMS (12/15/98) and agreed to by the Regional Office (2/4/99). Both letters are on file in the Security Office located on the third floor of Bldg. #3 (cabinet #3). POC is Iam Secure (401) 555-1234."

2.2 Safeguards

CAST serves as the repository for the Corrective Action Plan (see Section 3.5 of the CMS/Business Partners Systems Security Manual). When the Annual Self-assessment is conducted, those items recorded as "Partial," or "Planned" are considered to be the Corrective Action Plan. CAST entries for Partial or Planned items should include the following dates in the Explanation/ Comments field:

- Date a particular Safeguard can be procured or initiated.
- Dates of various stages of implementation.



Title:

Description:

Priority:

Total Safeguard Cost:

% Cost Applied to CMS: 100.00%

Responsibility: ● Generic ○ Shared System Maintainer

Safeguard Type

Safeguard cost to CMS for this contract:

Projected Recurring CMS Cost:

Figure A-3. Safeguard Cost Form

New Safeguards are developed when current hardware, software, facilities, personnel, or procedures are not sufficient to achieve compliance with a given CSR. While some Safeguards may require additional funding to implement, not all require funding. Funding may consist of corporate funding, **existing Line One** funding, and/or some other funding source. Not all Safeguards require **additional** funding. Many new Safeguards may already be funded through existing funding sources (such as by **Line One** requirements).

Recommendations for generating Safeguards:

- *Maintain the integrity of the Safeguard costs in relation to the CSR.*
- *Do not group disparate CSR costs into a single Safeguard.*
- *Provide separate Safeguard costs for different subcontracts.*
- *Do not rollup numerous CSRs into a single cost.*
- *Provide sufficient detail to enable evaluation of the total Safeguard cost and projected recurring costs.*

Safeguards are generated by selecting the "Safeguards" button on the CAST self-assessment form. New Safeguards may be developed or new Safeguards that have already been developed may be referenced (and edited) (see Figure A-3).

1) **Title:** This is the title of the proposed Safeguard. The title should be unique and easily identifiable with the content of the Safeguard description. Do not use CSR numbers or CSR titles to name Safeguards. Instead use some unique identifiers that are intuitive to both the business partner's organization as well as CMS. The Safeguard title should relate to the

Safeguard only, not to the CSRs that are addressed. An example of a reasonable CSR naming convention might be some unique number plus a noun-name.

Examples:

"SG001 - Purchase and implement virus protection software"

"SW002 - Purchase and install Network Encryption Software"

"HW003 - Install Firewall host for MVS system"

2) **Description:** This is a detailed description of the planned Safeguard. This will include all **details** of the Safeguard design, including equipment type, personnel requirements, job descriptions, work to be performed, etc. This section should be as detailed as possible as it will be used to justify cost. The costs described here represent the actual cost of all components of the Safeguard. The distribution of cost between the business partner and CMS will be addressed in a separate field. However, if this Safeguard will be utilized by more than one CMS contract (i.e., both a Part A and a Part B contract will utilize this Safeguard), describe the distribution of use by each contract here.

Example:

The firewall Safeguard will include:

• 1 Micro server with dual CPU	$4000.00
o NT 4.0 or Windows 2000 Server software	$500.00
o Configured with Maximum high-level protection	$500.00
• 1 Cisco router	$10,000.00
o Cisco Secure Policy software	$2,500.00
o Cisco Secure VPN client	$2,500.00
• Cisco Consulting Services	$5,000.00

This use of Safeguard will be distributed across Corporate uses, Part A, and Part B contracts. Corporate use will account for ~ 20% of volume. Part A will account for 70% volume and Part B will account for 10% volume.

3) **Priority:** This is the priority of this Safeguard as perceived by the user (business partner). The priority reflects the business importance to the business partner. Priorities should be incremental starting at 1 and ascending to the total number of Safeguards (i.e., 1 through 17 for a total of 17 Safeguards). One (1) is the highest priority.

4) **Total Safeguard cost:** This section will include the Total cost of the Safeguard for the first year of implementation. These will include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. Note: This submission will be used for budgetary purposes it must be as accurate as feasible. It is advised that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted.

5) **Projected Recurring Cost:** This is the projected recurring cost to CMS to maintain this Safeguard for the following FY. This includes depreciation, amortization, etc. Cost associated with continuing funding should be added to subsequent line one charges where applicable.

6) **% Cost Applied to CMS:** This is the percentage of cost of the Safeguard that will be charged to CMS. This is the percentage of cost that CMS will carry for Safeguards that will be shared between CMS (Medicare) systems and corporate systems.

7) **Safeguard Type:** This is the type of Safeguard that is planned. The user will choose from a drop-down list of Safeguard type that includes Outsource, Hardware, Software, Facilities, and/or Personnel. The Safeguard can be of any combination of one or more of the five possibilities.

8) **Responsibility:** This is a radio button that assigns responsibility to either the entity performing the self-assessment, or to the System Maintainer (for Shared Systems Software changes required to meet this CSR). Safeguards assigned to the standard system maintainer shall not be funded through the entity completing this self-assessment. However, these Safeguards will be reviewed and forwarded to the Shared System Maintainer, where applicable.

9) **Safeguard cost to CMS for this contract:** This is the system calculated (by CAST) cost to CMS for implementing this Safeguard. It is calculated using the following formula:

   (Total Safeguard cost) x (% Cost Applied to CMS) x (% CMS Cost Applied to this contract) = Total current FY CMS cost for this contract.

Appendix B
Medicare Information Technology (IT)
Systems Contingency Planning

3.0 Definition of an Acceptable Contingency Plan

(Rev. 4, 03-05-04)

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

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

Before developing an IT systems contingency plan, it is advisable to have or create a contingency policy. The contingency plan must be driven by a contingency policy. The contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

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

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

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

1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high quality service.
2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.
3. Considers risk assessment results.
4. Addresses possible and probable emergencies or system disruptions.
5. Can be sufficiently tested on an established regular basis at reasonable cost.

6. Contains information that is needed and useful during an emergency or system disruption.
7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.
8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.
9. Clearly defines the resources necessary to implement the plan.
10. Reflects what can be done – is not a wish list.
11. Assumes people will use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe pressure.
12. Addresses backup and alternate sites.
13. Addresses the use of manual operations, where appropriate and necessary.
14. Contains definitive "Call Lists" to use for contacting the appropriate persons in the proper sequence. This list would include vendor points of contact.

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

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

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

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

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

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

6.3 Test Types

(Rev. 4, 03-05-04)

Contingency plan test guidance suggests three types of testing:

- Walkthrough
- Simulation/modeling
- Live.

These are defined below:

- ***Walkthrough:*** *A walkthrough test is accomplished by going thorough a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented in a way that they can be logically followed. A "test team" might sit around a table and talk thorough each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but would not actually start all hardware, software and communication operations in order to assume the function of the primary site.*
- ***Simulation/Modeling:*** *Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster, or the number of people that can get to an alternate site following a disaster.*

  Simulation involves taking some physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team do the same a the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.
- ***Live:*** *This is the most complete and expensive test to accomplish. It involves doing physically what would actually be accomplished if an emergency occurred. People and materials would be moved to an alternate site for the test. Servers would actually be shut down to reduce capability. Power would actually be shut off. Live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is*

substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end):

- End-to-end testing *can* be done as part of walkthrough or live test.
- Not testing end-to-end means *that* some links, processes, or subsystems are missed.
    - What is the risk in not doing end-to-end?
- Live end-to-end testing can be very expensive!

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

6.3.1 Live vs. Walkthrough

(Rev. 4, 03-05-04)

- High-level testing can *take the form of* a walkthrough test.
- *A walkthrough c*an be part of the overall testing process, but not the whole process.
- Lower-level testing can *include a* walkthrough, if live testing *is not an option*.
    - *Live testing should be the f*irst choice.
    - Fall back to a simulation/model if live test*ing is not an option*.
        - Cost, time, and interruption of normal operations are major considerations in doing a live test.
    - *A* walkthrough test *should be the last resort*.
        - Ask what a walkthrough test *would* miss.
        - *Consider the ramifications of missing* that part of *the* test.
        - *Remember that t*here is risk in not doing a live test—*c*an the risk be accepted?
    - C*onsider the c*riticality of functions, processes, and systems.
        - If critical to continuing essential business operations, then these are strong candidates for live testing.
- *Testing i*nterfaces.
    - It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces *using* a “walkthrough” method. Simulation or “live” testing is preferred.
- *Cost and* complexity

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

6.3.2 End-to-End

(Rev. 4, 03-05-04)

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

- End-to-end testing must *only* be considered for critical functions, processes, or systems.
- Why is end-to-end testing needed?
  - *It p*rovide*s the best* assurance that there are no problems.
- Would a partial test be meaningful?
  - If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.
- Examples of types of end-to-end tests:
  - Claims receipt through to check generation;
  - Query of a data base through to the response;
  - MSP check request through to check issue and back to MSP.
- Evaluate complexity and cost.
  - The decision on how to test critical functions, processes, and systems must carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost out weighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.
- C*onsider the c*riticality of functions, processes, and systems.
  - Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.
- If you can’t do end-to-end testing, then consider live testing of all links possible to help ensure minimum problems.
  - Or, do simulation/modeling.
  - Or, do walkthrough.

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

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

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

7.0 Minimum Recovery Times

(Rev. 4, 03-05-04)

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

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

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

8.1 Business Partner Management

(Rev. 4, 03-05-04)

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary IT systems contingency planning.
- Ensures that appropriate contingency plans are developed, periodically tested, and maintained.
- Ensures that all IT operations participate in the contingency planning and the development of the plans.

- Reviews the plan and recommendations.
- Requests and/or provides funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the plan.
- Reviews test results.
- Ensures that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.
- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.
- Business partner management must approve:
    - The contingency plan
    - Changes to the contingency plan
    - Test Plans
    - Test Results
    - Corrective Action Plans*,*
    - Retest Plans*,*
    - Memos of Understanding/Formal Arrangement Documents
    - Changes *to* storage and backup/alternate site facilities.

11.0 Checklist

(Rev. 4, 03-05-04)

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

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

1. Introduction

   Does the contingency plan contain:

   - Background
       - Is a history of the plan provided? Are the physical environment and the systems discussed?
   - Purpose/Objective
       - What does the plan address? Why was it written? What is hoped to be accomplished by using the plan?

   - Management Commitment Statement
     - Has the contingency plan been approved by management and the SSO? Once the contingency plan is created, reviewed and ready for distribution, it should be approved by site, operations and IS management, and the SSO.
   - Scope
     - Are the boundaries of the plan indicated? What organizations are involved, not involved?
       - Organizations
       - Systems
       - Boundaries?
   - IT Capabilities and Resources
     - Is the focus of the plan on IT systems, capabilities, and resources?
   - Contingency Plan Policy
     - Priorities
     - Continuous operation
       - Are there functions, processes, or systems that are required to continue without interruption?
     - Recovery after short interruption
       - Which functions, processes, or systems can be interrupted for a short time?
       - Minimum Recovery Times
     - Are recovery times stated?
     - Standalone Units
       - Does a contingency plan exist for any standalone workstation? A key part of a contingency plan should address any standalone workstations that are part of the critical operations environment. It should state where backup software and support data for these workstations is stored.
   - Is the plan reviewed and approved by other key affected persons?

2. Assumptions
   - Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?
3. Authority/References
   - Who or what document is authorizing the creation of the contingency plan?
     - What are the key references that apply to the plan?
4. Definition of what the Contingency Plan Addresses
   - Organizations

  - To which organizations does the contingency plan apply?
- Systems
  - Is there a general description of systems and/or processes?
- *Boundaries*

5. *Three phases defined*

   Does the plan address three phases of emergency or system disruption?

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

6. Roles/Responsibilities Defined

   - Has the necessary contingency plan implementation organization been defined and the responsibilities of all those involved clearly stated with no ‘gray areas’?
   - Will all who have a task to perform be aware of what is expected of them?
   - Does the contingency plan assign responsibilities for recovery? The responsibilities of key management and staff persons should be carefully described in the contingency plan, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

   - Does the contingency plan address critical systems and processes?
   - Have emergency processing priorities been established and approved by management?
   - Does the contingency plan specify critical data? The contingency plan should specify the critical data needed to continue critical business functions and how frequently the data is backed up.
   - Has a list of critical operations, data, and applications been created? In preparation for preparing the contingency plan, a list of current critical operations, data and applications should be prepared and approved by management. These are what

would be needed to continue the critical business functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.
- Does the contingency plan address issues relative to pre-planned alternate locations? The contingency plan must address any potential issues relative to pre-planned alternate locations. These include:
    - insurance
    - equipment replacement
    - phones
    - utilities
    - security.
- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities should include:
    - prioritizing operations
    - identifying key personnel and how to reach them
    - listing backup systems and where they are located
    - stocking critical forms, blank check stock and supplies off-site
    - developing reliable sources for replacing equipment on an emergency basis.
- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?
- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?
- Have temporary data storage sites and location of stored backups been identified?
- Is the frequency of file backup documented?
- Have the arrangements been made for ensuring continuing communications capabilities?
- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
- Is system, application and other key documentation maintained at the off-site location?

- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?
- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.
- Is the contingency plan stored off-site at alternate/backup locations? Copies of the contingency plan should be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the contingency plan that are stored in a private home must be protected from inadvertent access.

9. Required Resources
    - Are the following resources for supporting critical operations defined and available for an emergency?
        - Hardware
        - Software
        - Communications
        - Data
        - Documents
        - Facilities
        - People
        - Supplies
        - Basic essentials (water, food, shelter, transportation, etc.)
    - Does the contingency plan provide for backup personnel? As the contingency plan is implemented, it is necessary to have additional people available to support recovery operations. The contingency plan should specify who these people are and when they would normally be called into action.
10. Training
    - Is management and staff trained to respond to emergencies? Security training should include modules for management and staff relative to their roles for handling emergency situations.
11. Testing the Contingency Plan
    - Is there a section in the contingency plan that addresses testing of the plan?
    - Testing of the contingency plan should address the following topics:
        - Test Philosophy
        - Test Plans

    - Boundaries
    - Live vs. Walkthrough vs. End-to-End Testing
    - Test Reports
    - Responsibilities.

12. Contingency Plan Maintenance

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

13. Relationships/Interfaces

- Does the contingency plan identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.
- Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?
- Is the plan compatible with plans of interacting organizations and systems?
- What internal interfaces must be considered?
- Is the plan compatible with plans of interacting organizations and systems?
- Which corporate interfaces must be considered?
- Are there special interfaces with corporate systems that must be addressed in the contingency plan?

14. Attachments

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

A. Actions for Each Phase

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

B. Procedures

- Are there detailed instructions for:
    - responding to emergencies?
    - recovering?
    - restoring operations?
- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency should be in place.

- Are there procedures for addressing the situation where the processing site is intact, but people can’t get to it because of a natural disaster? Can the business be operated remotely?
- Is there an implementation plan for working from home?

C. Call Trees

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

D. Hardware Inventory

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

E. Software Inventory

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

F. System Descriptions

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

G. Alternate/Backup Site Information

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

H. Assets/Resources

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

I. Risk Assessment Summary

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

J. Agreements/Memo of Understanding

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

K. Manual Operations

- Are manual operating procedures in place so that certain functions can be continued manually if automated support is not available soon enough?
- Manual processing procedures should exist because in the backup phase, until automated capabilities can take over the information processing, it may be necessary to use manual processing. Provisions should be made to provide this manual capability.

L. Supplies/Materials/Equipment

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

M. Floor Plans

- Are the necessary floor plans available?

N. Maps

- Are the necessary area and street maps available?

Appendix C
An Approach to Fraud Control

(Rev. 4, 03-05-04)

1.*0* Introduction

(Rev. 4, 03-05-04)

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

2.*0* Safeguards Against Employee Fraud

(Rev. 4, 03-05-04)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These are consistent with the CMS Core Security Requirements outlined in Appendix A of the CMS/Business Partners Systems Security Manual and do not constitute wholly different or additional minimum requirements. The following countermeasures should prove especially effective against currently prevalent fraudulent activities and are discussed primarily as they relate to prevention/detection of fraud.

A. Screen New Employees

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

Any blatant dishonesty in the application (such as claiming qualifications and experience the applicant never had) should remove the applicant from further consideration. Check references and crosscheck them (one against the other) for consistency as well as content.

Evaluate them on the basis of the contact's personal knowledge of the applicant's job-related qualifications and integrity.

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

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

Ask former employers as well as the applicant, whether the employee was ever bonded, or was ever refused bonding. Sensitive screening should not result in violating an applicant's civil rights, while assuring you (and your bonding company) that prudent concern is exercised in the hiring process.

B. Bonding

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

C. Separation of Duties

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

D. Rotation of Duties

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

E. Manual Controls

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

F. Training

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

G. Notices

Notices, both periodic and situational, are effective and necessary in the prevention and control of fraud. It is not enough to formulate management policy, or to conduct employee training relative to fraudulent activity. It is possible to remind employees of management's continuing concerns and to evaluate employee awareness through simple reminders or announcements of what is happening relative to fraud controls (of a general nature) and management's reliance on their cooperation and understanding of their responsibilities. Without this evidence of sustained management commitment, policy utterances tend to fade from memory or become regarded as part of a new employee's orientation and not part of the scene. This is true of minor abuses, but is also true of abuses that escalate into fraud.

H. Automatic Controls

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

I. Audit Routines

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

3.*0* Checklist for Medicare Fraud

(Rev. 4, 03-05-04)

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

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

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

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

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

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

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

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

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

9) Are audit trails generated *that* identify employees creating inputs or making adjustments/corrections that would pinpoint responsibility for any fraudulent act?

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

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

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

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

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

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

16) Does management insist on integrity at all levels?

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

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

19) Are alternative fraud controls invoked during emergencies?

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

21) Are fraud audits conducted both periodically and randomly?

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

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

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

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

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

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

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

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

30) Are special fraud controls specified for backup operations?

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

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

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

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

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

Appendix E :
Glossary

(Rev. 4, 03-05-04)

	Definition
Access	(1) A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (NCSC-TG-004) (2) Opportunity to make use of an information system (IS) resource. (NSTISSI)
Access Control	Controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access controls include both physical access controls, which limit access to facilities and associated hardware, and logical controls, which prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically. (FISCAM)
Access Control Facility	*An access control software package marketed by Computer Associates International, Inc. (FISCAM)*
Access Control Software	This type of software (CA-ACF2, RACF, CA-TOP SECRET), which is external to the operating system, provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a wanting, or allowing access to all resources without warning regardless of authority. (FISCAM)
Access Method	The technique used for selecting records in a file for processing, retrieval, or storage. (FISCAM)
Access Path	(1) The path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc. (FISCAM) (2) Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path.

Term	Definition
Access Privileges	*Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on the system, and under what circumstances this access will be allowed. (FISCAM)*
Accountability	The existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established. (FISCAM)
Accreditation	(1) The official management authorization for the operation on an application and is based on the certification process as well as other management considerations. (AISSP) (FIPS PUB 102) (2) A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (NCSC-TG-004)
Application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. (FISCAM)
Application Controls	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. (FISCAM)
Application Programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities. (FISCAM)
Application Programs	See Application.
Application System(s)	*A computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system. (AISSP) (FIPS PUB 11-3)*
Application System Manager	See Application Manager.

Term	Definition
Asset	Any software, data, hardware, administrative, physical communications, or personnel resource within an ADP system of activity.
Attack	*The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (NCSC-TG-004)*
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (NSTISSI)
Audit Software	*Generic audit software consists of a special program or set of programs designed to audit data stored on computer media. Audit software performs functions such as data extraction and reformatting, file creation, sorting, and downloading. This type of audit software may also be used to perform computations, data analysis, sample selection, summarization, file stratification, field comparison, file matching, or statistical analysis. The term audit software may also refer to programs that audit specific functions, features, and controls associated with specific types of computer systems to evaluate integrity and identify security exposures. (FISCAM)*
Audit Trail	In an accounting package, any program feature that automatically keeps a record of transactions so you can backtrack to find the origin of specific figures that appear on reports. In computer systems, a step-by-step history of a transaction, especially a transaction with security sensitivity. Includes source documents, electronic logs, and records of accesses to restricted files. (FISCAM)
Authentication	The act of verifying the identity of a user and the user's eligibility to access computerized information. Designed to protect against fraudulent activity. (FISCAM)
Automated Information System (AIS)	The organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. (AISSP) (OMB Circular A-130)

Term	Definition
Automated Information Systems Security	See Systems Security.
Backup	Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource. (FISCAM)
Backup Plan	See Contingency Plans.
Backup Procedures	*A regular maintenance procedure that copies all new or altered files to a backup storage medium, such as a tape drive. (FISCAM)*
Batch (Processing)	A mode of operation in which transactions are accumulated over a period of time, such as a day, week, or month and then processed in a single run. In batch processing, users do not interact with the system while their programs and data are processing as they do during interactive processing. (FISCAM)
Biometric Authentication	The process of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometric devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. (FISCAM)
Breach(es)	The successful and repeatable defeat of security controls with or without an arrest, which if carried to consummation, could result in a penetration of the system. Examples of breaches are: 1. Operation of user code in master mode. 2. Unauthorized acquisition of identification password or file access passwords. 3. Accessing a file without using prescribed operating system mechanisms. 4. Unauthorized access to tape library.
Browsing	(1) The act of electronically perusing files and records without authorization. (FISCAM) (2) The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (NCSC-TG-004)

Term	Definition
Business Partners	Non-federal personnel who perform services for the federal government at a site owned by the partner under the terms and conditions of a contractual agreement. Business partners need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements. CMS business partners are Shared Systems Maintainers (SSM), CWF host sites, DMERC, Data Centers and other specialty contractors.
Certification (Recertification)	(1) Consists of a technical evaluation of a sensitive application to see how well it meets security requirements. (AISSP) (FIPS PUB 102) (2) A formal process by which an agency official verifies, initially or by periodic reassessment, that a system's security features meet a set of specified requirements.
Checkpoint	The process of saving the current state of a program and its data, including intermediate results to disk or other nonvolatile storage, so that if interrupted the program could be restarted at the point at which the last checkpoint occurred. (FISCAM)
Chief Information Officer (CIO)	The **CIO** is responsible for the implementation and administration of the AIS Security Program within an organization.
Cipher Key Lock	*A lock with a key pad-like device that requires the manual entry of a predetermined code for entry. (FISCAM)*
Classified Resources/ Data/Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (NSTISSI)
Code	Instructions written in a computer programming language. (See object code and source code.) (FISCAM)
Cold Site	An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative computing location. (FISCAM)

Term	Definition
Command(s)	A job control statement or a message, sent to the computer system, that initiates a processing task. (FISCAM)
Communications Program	*A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks. (FISCAM)*
Communications Security (COMSEC)	Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (NSTISSI)
Compact Disc-Read Only Memory (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally read-only. (FISCAM)
Compatibility	The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are key to achieving compatibility. (FISCAM)
Compensating Control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions. (FISCAM)
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components. (FISCAM)
Compromise	An unauthorized disclosure or loss of sensitive defense data. (FIPS PUB 39)
Computer	See Computer System.
Computer Facility	A site or location with computer hardware where information processing is performed or where data from such sites are stored. (FISCAM)
Computer Network	See Network.
Computer Operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems. (FISCAM)

Term	Definition
Computer-related Controls	*Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications. (FISCAM)*
Computer Resource	See Resource.
Computer Room	Room within a facility that houses computers and/or telecommunication devices. (FISCAM)
Computer Security	See Information Systems Security and Systems Security.
Computer Security Incident Response Capability (CSIRC)	That part of the computer security effort that provides the capability to respond to computer security threats rapidly and effectively. [A CSIRC provides a way for users to report incidents, and it provides personnel and tools for Investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents.] (AISSP) (Source: NIST SPEC PUB 800-3)
Computer System	(1) A complete computer installation, including peripherals, in which all the components are designed to work with each other. (FISCAM) (2) Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (AISSP) (Computer Security Act of 1987)
Confidentiality	Ensuring that transmitted or stored data are not read by unauthorized persons. (FISCAM)
Configuration Management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. (FISCAM)
Console	Traditionally, a control unit such as a terminal through which a user Communicates with a computer. In the mainframe environment, a **Console** is the operator's station. (FISCAM)

Term	Definition
Consortium	Currently consists of four CMS offices (Northeastern, Southern, Midwestern, and Western) that oversee the operations at the Regional Offices.
Consortium Contractor Management Officer (CCMO)	Part of the Regional Consortiums, the **CCMO** is responsible for leading and directing contractor management at the consortium level.
Contingency Plan(s)	(1) Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster. (FISCAM) (2) A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (AISSP) (FIPS PUB 11-3)
Contingency Planning	(1) The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. (ISSPH - Glossary) (2) See contingency plan. (FISCAM)
Contractors	Non-federal personnel who perform services for the federal government under the terms and conditions of a contractual agreement. Contractors need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.
Control Technique	Statements that provide a description of what physical, software, procedural or people related condition must be met or in existence in order to satisfy a core requirement. (Appendix A.)
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text or plain text and other data are transformed into coded form by encryption and translated back to plain text or data by decryption. (FISCAM)
Data	Facts and information that can be communicated and manipulated. (FISCAM)
Data Administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. (FISCAM)
Data Center	See Computer Facility.

Term	Definition
Data Communications	(1) The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM) (2) The transfer of data between functional units by means of data transmission according to a protocol. (AISSP) (FIPS PUB 11-3)
Data Control	The function responsible for seeing that all data necessary for processing is present and that all output is complete and distributed properly. This function is generally responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing. (FISCAM)
Data Dictionary	A repository of information about data, such as its meaning, relationships to other data, origin, usage, and format. The dictionary assists company management, database administrators, systems analysts, and application programmers in effectively planning, controlling, and evaluating the collection, storage, and use of data. (FISCAM)
Data Encryption Standard (DES)	(1) A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data. (FISCAM) (2) The National Institute of Standards and Technology **Data Encryption Standard** was adopted by the U.S. Government as Federal Information Processing Standard (FIPS) Publication 46 [at publication 46-1], which allows only hardware implementations of the data encryption algorithm. (AISSP) (FIPS PUB 11-3)
Data File	See File.
Data Owner	*See "Owner." (FISCAM)*
Data Processing	The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing. (FISCAM)
Data Security	(1) The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (FIPS PUB 39) (2) See Security Management Function.
Data Validation	Checking transaction data for any errors or omissions that can be detected by examining the data. (FISCAM)

Term	Definition
Database	(1) A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer. (FISCAM) (2) A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (AISSP) (FIPS PUB 11-3)
Database Administrator (DBA)	*The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database. (FISCAM)*
Database Management (DBM)	Tasks related to creating, maintaining, organizing, and retrieving information from a database. (FISCAM)
Database Management System (DBMS)	A software product (DB2, IMS, IDMS) that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions, such as queries or updates from users, and permit centralized control of security and data integrity. (FISCAM)
DBMS	See Database Management System.
Debug (Software)	To detect, locate, and correct logical or syntactical errors in a computer program. (FISCAM)
Degauss	To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (FIPS PUB 39)
Denial of Service (DOS)	Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Synonymous with interdiction. (NCSC-TG-004)
DES	See Data Encryption Standard.

Term	Definition
Dial-up(in) Access	A means of connecting to another computer or a network like the Internet, over a telecommunications line using a modem-equipped computer. (FISCAM)
Dial-up Security Software	*Software that controls access via remote dial-up. One method of preventing unauthorized users from accessing the system through an unapproved telephone line is through dial-back procedures in which the dial-up security software disconnects a call initiated from outside the network via dial-up lines, looks up the user's telephone number, and uses that number to call the user. (FISCAM)*
Disaster Plan	See Contingency Plan.
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (FISCAM)
Disclosure (Illegal Access and Disclosure)	Activities of employees that involve improper systems access and sometime disclosure of information found thereon, but not serious enough to warrant criminal prosecution. These cases should be entered on the Fraud Monitoring and Reporting System.
Disk Storage	*High-density random access magnetic storage devices that store billions of bits of data on round, flat plates that are either metal or plastic. (FISCAM)*
Diskette	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case. (FISCAM)
Electronic Data Interchange (EDI)	*A standard for the electronic exchange of business documents, such as invoices and purchase orders. Electronic data interchange (EDI) eliminates intermediate steps in processes that rely on the transmission of paper-based instructions and documents by performing them electronically, computer to computer. (FISCAM)*

Term	Definition
Electronic Mail (e-mail)	The transmission of memos and messages over a network. Within an enterprise, users can send mail to a single recipient or broadcast it to multiple users. With multitasking workstations, mail can be delivered and announced while the user is working in an application. Otherwise, mail is sent to a simulated mailbox in the network server or host computer, which must be interrogated. An e-mail system requires a messaging system, which provides the store and forward capability, and a mail program that provides the user interface with send and receive functions. The Internet revolutionized e-mail by turning countless incompatible islands into one global system. The Internet initially served its own members, of course, but then began to act as a mail gateway between the major online services. It then became "the" messaging system for the planet. (TechEncy)
Electronic Signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. (FISCAM)
Encryption	The transformation of data into a form readable only by using the appropriate key held only by authorized parties. (FISCAM)
End User(s)	Employees who have access to computer systems and networks that process, store, or transmit information. This is the largest and most heterogeneous group of employees. It consists of everyone, from an executive with a desktop system to application programmers to data entry clerks.
Environmental Controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls. (FISCAM)
Exception Criteria	Exception criteria refers to batch processes that return files or records as not meeting certain predefined criteria for processing.

Term	Definition
Execute (Access)	This level of access provides the ability to execute a program. (FISCAM)
Facility(ies)	See Computer Facility.
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record. (FISCAM)
File	A collection of records stored in computerized form. (FISCAM)
Firewall	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. (FISCAM)
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. (FISCAM)
General Controls	The structure, policies, and procedures that apply to an entity's overall computer operations. They include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls. (FISCAM)
General Support System(s) (GSS)	(1) An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a **general support system** is to provide processing or communication support. (FISCAM) (2) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (OMB Circular A-130)

Term	Definition
Guided Media	(1) Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable) (2) Provides a closed path between sender and receiver • Twisted Pair (e.g. Telephone cable) • Coaxial Cable • Optical Fiber (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
Handled	(As in "Data handled.") Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.
Hardware	The physical components of information technology, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. (FISCAM)
Hot Site	*A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster. (FISCAM)*
Image	An exact copy of what is on the storage medium
Implementation	The process of making a system operational in the organization. (FISCAM)
Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.
Information	(1) The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people. (FISCAM) (2) Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (AISSP) (OMB Circular A-130)
Information Resource	See Resource.
Information Resource Owner	See Owner.

Term	Definition
Information Systems (IS)	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (NSTISSI)
Information Systems Security (INFOSEC)	The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including cryptosecurity, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (AISSP) (NISTIR 4659) (Also see Systems Security)
Information Systems Security Officer (ISSO)	(1) Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer. (NSTISSI)
Information Technology (IT)	(1) Processing information by computer. (TechEncy) (2) IT or Information Technology has probably been the most redefined term over the past few years. The definition has varied from simple automation of manual processes using micro-processors to computers to networks to desktop publishing to networking. (Source: U. Texas)
Initial Program Load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program. (FISCAM)
Input	Any information entered into a computer or the process of entering data into the computer. (FISCAM)
Integrity	With respect to data, its accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users. (FISCAM)
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user. (FISCAM)

Term	Definition
Internal Control	A process, effected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. **Internal control** also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring. (Also referred to as Internal Control Structure) (FISCAM)
Internet	When capitalized, the term "**Internet**" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
Investigation(s)	The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system.
IPL	See Initial Program Load.
Job	A set of data that completely defines a unit of work for a computer. A **job** usually includes programs, linkages, files, and instructions to the operating system. (FISCAM)
Junk Mail (e-mail)	Transmitting e-mail to unsolicited recipients. U.S. federal law 47USC227 prohibits broadcasting junk faxes and e-mail, allowing recipients to sue the sender in Small Claims Court for $500 per copy. (TechEncy)
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message. (FISCAM)
Key Management	Supervision and control of the process whereby a key is generated, stored, protected, transferred, loaded, used, and destroyed. (NSTISSI)

Term	Definition
Keystroke Monitoring	A process whereby computer system administrators view or record both the keystrokes entered by a computer user and the computer's response during a user-to-computer session. (AISSP – Source: CSL Bulletin)
Library	In computer terms, a **library** is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a **library**, each program is called a member. **Libraries** are also called partitioned data sets (PDS). **Library** can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape **libraries**. (FISCAM)
Library Control/Management	The function responsible for controlling program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. (FISCAM)
Library Management Software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes. (FISCAM)
Life-Cycle Process **Life-Cycle Model**	(1) Spans the entire time that a project/program including hardware and software is being planned, designed, developed, procured, installed, used, and retired from service. (2) A framework containing the processes, activities and tasks involved in the development, operation and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use. (Source: ISO/IEC 12207)
Limited Background Investigation (LBI)	This investigation consists of a NACI, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years. (SSPS&GH - Glossary)
Load Library	A partitioned data set used for storing load modules for later retrieval. (FISCAM)
Load Module	The results of the link edit process. An executable unit of code loaded into memory by the loader. (FISCAM)

Term	Definition
Local Area Network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. **Local area networks** commonly include microcomputers and shared (often-expensive) resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks. (FISCAM)
Log(s)	With respect to computer systems, to record an event or transaction. (FISCAM)
Log Off	The process of terminating a connection with a computer system or peripheral device in an orderly way. (FISCAM)
Log On (Log In)	The process of establishing a connection with, or gaining access to, a computer system or peripheral device. (FISCAM)
Logging File	See Log above.
Logic Bomb	In programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. (FISCAM)
Logical Access Control	The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges. (FISCAM)
Mail Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system. (TechEncy)
Mainframe System (Computer)	A multi-user computer designed to meet the computing needs of a large organization. The term came to be used generally to refer to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations. (FISCAM)
Maintenance	(1) Altering programs after they have been in use for a while. **Maintenance** programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time. (FISCAM) (2) The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions. (Source: IEEE Std 610.12-1990)

Term	Definition
Major Application (MA)	(1) OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application. (FISCAM) (2) An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A major application can be either a major software application or a combination of hardware/software. Its sole purpose is to support a specific mission-related function. (ISSPH - Glossary) (3) An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB Circular A-130) All "Major Applications" require "special management attention." The System Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.
Malicious Software (Code)	The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (AISSP – Source: DHHS Definition, adapted from NIST SPEC PUB 500-166)

Term	Definition
Management Controls	*The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used consistent with the organization's mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision-making. (FISCAM)*
Master Console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands. (FISCAM)
Master File(s)	*In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period. (FISCAM)*
Material	Refers to data processed, stored, or used in and information generated by an ADP system regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements.
Media	The physical object such as paper, PC, and workstation diskettes, CD-ROMs, and other forms by which CMS data is stored or transported. The risk to exposure is considered greater when data is in an electronically readable and transmittable form than when the same data is in paper-only form. This is due to the greater volume of information that can be sent in electronic form, the ease and convenience with which the information can be transmitted, and the potential that such information will be intercepted or inadvertently sent to the wrong person or entity.
Methodology	The specific way of performing an operation that implies precise deliverables at the end of each stage. (TechEncy)
Migration	A change from an older hardware platform, operating system, or software version to a newer one. (FISCAM)
Minimum Background Investigation (MBI)	This investigation includes a NACI, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. The MBI is an enhanced version of the NACIC and can be used for selected public trust positions.

Term	Definition
Mission Critical	Vital to the operation of an organization. In the past, mission critical information systems were implemented on mainframes and minicomputers. Increasingly, they are being designed for and installed on personal computer networks. (TechEncy)
Misuse of Government Property	The use of computer systems for other than official business that does not involve a criminal violation but is not permissible under CMS policies.
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received. (FISCAM)
Modification	Loss of integrity of an asset or asset group through the intentional or unintentional alteration of the asset or asset group.
National Agency Check (NAC)	An integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary.
Need-To-Know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. (NSTISSI)
Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. *(FISCAM)*
Non-privileged Access	Cannot bypass any security controls.
Object Code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program. (FISCAM)

Term	Definition
Office of Information Services (OIS)	CMS Office that ensures the effective management of CMS's information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.
On-line	Available for immediate use. It typically refers to being connected to the Internet or other remote service. When you connect via modem, you are online after you dial in and log on to your Internet provider with your username and password. When you log off, you are offline. With cable modem and DSL service, you are online all the time. A peripheral device (terminal, printer, etc.) that is turned on and connected to the computer is also online. (TechEncy)
Operating System(s) (OS)	*The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running. (FISCAM)*
Operational Controls	*These controls relate to managing the entity's business and include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards, and (3) does what management directs it to do. (FISCAM)*
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy. (FISCAM)
Output Devices	*Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system. (FISCAM)*
Owner	Manager or director with responsibility for a computer resource, such as a data file or application program. (FISCAM)
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs. (FISCAM)
Passwords	(1) A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) (2) Most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications is often easy to circumvent if the user has access to the operating system (and knowledge of what to do).

Term	Definition
PDS	See Partitioned Data Set.
Penetration	Unauthorized act of bypassing the security mechanisms of a system. (NSTISSI)
Penetration Test	An activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.
Peripheral	*A hardware unit that is connected to and controlled by a computer, but external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer. (FISCAM)*
Personnel Controls	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause. (FISCAM)
Personal Data	Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
Personnel Security	Refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access. (AISSP – Source: NISTIR 4659) (Also see Personnel Controls)
Physical Access Control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment. (FISCAM)
Physical Security	Refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (SSPS&GH - Glossary) (Source: NISTIR 4659) (Also see Physical Access Control)

Term	Definition
Port	An interface between the CPU of the computer and a peripheral device that governs and synchronizes the flow of data between the CPU and the external device. (FISCAM)
Privacy Information	The individual's right to privacy must be protected in Federal Government information activities involving personal information. Such information is to be collected, maintained, and protected so as to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. (OMB Circular A-130)
Privileged Access	Can bypass, modify, or disable the technical or operational system security controls.
Privileges	Set of access rights permitted by the access control system. (FISCAM)
Probe	Attempt to gather information about an IS or its users. (NSTISSI)
Processing	The execution of program instructions by the computer's central processing unit. (FISCAM)
Production Control	The function responsible for monitoring the information into, through, and scheduling and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task. (FISCAM)
Production Environment	The system environment where the agency performs its operational information processing activities. (FISCAM)
Production Programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management. (FISCAM)
Profile	A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. (See Standard Profile and User Profile.) (FISCAM)
Program	A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system program, source programs, and object programs are all software programs. (FISCAM)
Program Library	See Library.

Term	Definition
Programmer	A person who designs, codes, tests, debugs, and documents computer programs. (FISCAM)
Programming Library Software	*A system that allows control and maintenance of programs for tracking purposes. The systems usually provide security, check out controls for programs, and on-line directories for information on the programs. (FISCAM)*
Project Officer	CMS official (generally located in Central Office business components) responsible for the oversight of other business partners. These include Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased. (FISCAM)
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data. (FISCAM)
Public Access Controls	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records. (FISCAM)
Public Domain Software	Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances. (FISCAM)
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke Public key certificates accommodating a variety of security Technologies, including the use of software. (NSTISSI)
Public Trust Positions	Positions that have the potential for action or inaction by their incumbents to affect the integrity, efficiency, or effectiveness of assigned Government activities. The potential for adverse effects includes action or inaction that could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. (Source: 5 CFR Part 731)

Term	Definition
Quality Assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures, and (2) the software meets the functional specifications defined by the user. (FISCAM)
Read Access	This level of access provides the ability to look at and copy data or a software program. (FISCAM)
Real-time System	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed. (FISCAM)
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item. (FISCAM)
Recovery Procedures	Actions necessary to restore data files of an IS and computational capability after a system failure. (NSTISSI)
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior. (FISCAM)
Remote Access	The process of communicating with a computer located in another place over a communications link. (FISCAM)
Resource(s)	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and non-computerized records. (FISCAM)
Resource Access Control Facility (RACF)	*An access control software package developed by IBM. (FISCAM)*
Resource Owner	See Owner. *(FISCAM)*
Review and Approval	The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network.

Term	Definition
Risk	The potential for harm or loss is best expressed as the answers to these four questions: What could happen? (What is the threat?) How bad could it be? (What is the impact or consequence?) How often might it happen? (What is the frequency?) How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" per se. (HISM)
Risk Analysis	(1) The identification and study of the vulnerability of a system and the possible threats to its security. (AISSP – Source: FIPS PUB 11-3) (2) This term represents the process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures. (HISM)
Risk Assessment	(1) The identification and analysis of possible risks in meeting the agency's objectives that forms a basis for managing the risks identified and implementing deterrents. (FISCAM) (2) This term represents the assignment of value to assets, threat frequency (annualized), consequence (i.e., exposure factors), and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied. The term risk assessment is used to characterize both the process and the result of analyzing and assessing risk. (HISM)
Risk Evaluation	This task includes the evaluation of all collected information regarding threats, vulnerabilities, assets, and asset values in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur. Results are usually expressed in monetary terms on an annualized basis (ALE) or graphically as a probabilistic "risk curve" for a quantitative risk assessment. For a qualitative risk assessment, results are usually expressed through a matrix of qualitative metrics such as ordinal ranking (low, medium, high, or 1, 2, 3). (HISM)

Term	Definition
Risk Management	(1) A management approach designed to reduce risks inherent to system development and operations. (FISCAM) (2) The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (AISSP – Source: NISTIR 4659) (3) This term characterizes the overall process. The first, or risk assessment, phase includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk. The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process of ever-increasing complexity. (HISM)
Resource	Any agency Automated Information System (AIS) asset. (AISSP – Source: DHHS Definition)
Router	An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route. (FISCAM)
Rules of Behavior	Rules for individual users of each general support system or application. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training. (OMB Circular A-130)
Run	A popular, idiomatic expression for program execution. (FISCAM)
Run Manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. (FISCAM)
Safeguard	This term represents a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats. Safeguards are also often described as controls or countermeasures. (HISM)

Term	Definition
Sanction	Sanction policies and procedures are actions taken against employees who are non-compliant with security policy.
SDLC methodology	See System Development Life Cycle Methodology.
Security	The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability. (FISCAM)
Security Administrator (SA)	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks. (FISCAM)
Security Awareness	*(1) Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. (NIST SP 800-16)* *(2) Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences. (NIST SP 800-50)*
Security Certification	A formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications. To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system. (NIST Special Publication 800-12)
Security Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

Term	Definition
Security Level Designation	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse) and the operational criticality of data processing capabilities (i.e., the consequences were data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an AIS is assigned for the overall security level designation. (AISSP – Source: DHHS Definition)
Security Management Function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness. (FISCAM)
Security Plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. (FISCAM)
Security Policy	The set of laws, rules, and practices that regulate how an Organization manages, protects, and distributes sensitive information. (NCSC-TG-004)
Security Profile	See Profile.
Security Program	An entitywide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. (FISCAM)
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (NSTISSI)
Security Requirements Baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security. (NSTISSI)

Term	Definition
Security Software	See Access Control Software.
Security Training	*(1) Security training teaches people the [security] skills that will enable them to perform their jobs more effectively. (NIST SP 800-16)* *(2) Training strives to produce relevant and needed security skills and competencies. (NIST SP 800-50)*
Sensitive Application	An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (AISSP – Source: OMB Circular A-130)
Sensitive Data	Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (AISSP – Source: OMB Circular A-130)

Term	Definition
Sensitive Information	(1) Any information that, if lost, misused, or accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. (FISCAM) (2) **A**ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (AISSP – Source: Computer Security Act of 1987) (3) **A**ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under E-Mail 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987)
Sensitivity of Data	The need to protect data from unauthorized disclosure, fraud, waste, or abuse.
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network. (FISCAM)
Service continuity controls	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (FISCAM)
Significant Change	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (AISSP – Source: DHHS Definition)

Term	Definition
Single Loss Expectancy (SLE)	This value is classically derived from the following algorithm to determine the monetary loss (impact) for each occurrence of a threatened event: **ASSET VALUE X EXPOSURE FACTOR =** The SLE is usually an end result of a business impact analysis (BIA). A BIA typically stops short of evaluating the related threats' ARO or its significance. The SLE represents only one element of risk, the expected impact, monetary or otherwise, of a specific threat event. Because the BIA usually characterizes the massive losses resulting from a catastrophic event, however improbable, it is often employed as a scare tactic to get management attention and loosen budgetary constraints, often unreasonably. (HISM)
Smart Card	A credit card sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services. (FISCAM)
SMF	See System Management Facility.
Sniffer	Synonymous with packet **sniffer**. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text. (FISCAM)
Software	A computer program or programs, in contrast to the physical environment on which programs run (hardware). (FISCAM)
Software Life Cycle	The phases in the life of a software product, beginning with its conception and ending with its retirement. These stages generally include requirements analysis, design, construction, testing (validation), installation, operation, maintenance, and retirement. (FISCAM)
Software Security	General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system. (NCSC-TG-004)
Source Code	Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable. (FISCAM)
Special Management Attention	Some systems require "**special management attention**" to security due to the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access to, or modification of the information in the system. (OMB Circular A-130)

Term	Definition
SSPS&G Handbook	Systems Security Policy Standards and Guidelines Handbook
Stand-alone System (Computer)	A system that does not require support from other devices or systems. Links with other computers, if any, are incidental to the system's chief purpose. (FISCAM)
Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development. (FISCAM)
Standard Profile	A set of rules that describes the nature and extent of access to each resource that is available to a group of users with similar duties, such as accounts payable clerks. (FISCAM)

Term	Definition
System	(1) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (OMB Circular A-130) (2) Refers to a set of information resources under the same management control that share common functionality and require the same level of security controls. • The phase "General Support Systems (GSS)" as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications (MA)," as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, control software, or software for command and control). By categorizing both "General Support Systems" and "Major Applications" as "systems", unless explicitly stated, the procedures and guidance can address both in a simplified manner. • When writing the required System Security Plans, two formats are provided--one for General Support Systems, and one for Major Applications. This ensures that the differences for each are addressed (CMS, System Security Plans (SSP) Methodology , July 2000, SSPM. • A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system's hardware may include mainframe systems, desktop systems (e.g., PC's, Macintoshes, laptops, handheld devices), workstations and servers (e.g., Unix, NT, NC), local area networks (LAN), and any other platform regardless of the operating system.
System Administrator	The person responsible for administering use of a multi-user computer system, communications system, or both. (FISCAM)
System Analyst	A person who designs a system. (FISCAM)
System Development Life Cycle (SDLC) Methodology	The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle. (FISCAM)

Term	Definition
System Life Cycle	(1) The period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The system life cycle is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase. (AISSP – Source: FIPS PUB 101) (Also see Software Life Cycle)
System Management Facility	An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage. (FISCAM)
System Manager (SM)	The official who is responsible for the operation and use of an automated information system. (AISSP – Source: DHHS Definition)
System Programmer	A person who develops and maintains system software. (FISCAM)
System Software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software. (FISCAM)
System Testing	Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specification. (FISCAM)
System Security (Computer Security)	Refers to the concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss. (AISSP – Source: FIPS PUB 11-3)
System Security Administrator (SSA)	The person responsible for administering security on a multi-user computer system, communications system, or both.
Systems Security Incidents (Breaches)	Those incidents not classified as physical crimes, criminal violations, fraudulent activity, illegal access and disclosure or misuse of government property. A systems security breach is any action involving a system, which, if not corrected, could violate the provisions of the Privacy Act, Copyright laws, or CMS security policy or lead to a fraudulent act or criminal violation through use of an CMS system.

Term	Definition
Systems Security Coordinator (SSC)	Term used to designate the security officer in the 1992 ROM, MIM, and MCM. This business partner security officer had complete oversight and responsibility for all aspects of the security of the Medicare program.
System Security Officer (SSO)	The position held by the business partner Security Officer with complete oversight and responsibility for all aspects of the security of the Medicare program.
Systems Security Plan (SSP)	Provides a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (AISSP) (OMB Bulletin 90-08) (Also see IS Security Plan and System Security Plan)
System Security Profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS. (NSTISSI)
Tape Library	The physical site where magnetic media is stored. (FISCAM)
Tape Management System	*Software that controls and tracks tape files. (FISCAM)*
Technical Controls	See Logical Access Control.
Telecommunications	A general term for the electronic transmission of information of any type, such as data, television pictures, sound, or facsimiles, over any medium, such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM)
Terminal	A device consisting of a video adapter, a monitor, and a keyboard. (FISCAM)
Threat	(1) Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (NCSC-TG-004) (2) This term defines an event (e.g., a tornado, theft, or computer virus infection), the occurrence of which could have an undesirable impact. (HISM)
Threat Analysis	(1) The examination of all actions and events that might adversely affect a system or operation. (NCSC-TG-004) (2) This task includes the identification of threats that may adversely impact the target environment. (HISM)
Token	In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The **token** itself is not sufficient; the user must also be able to supply something memorized, such as a personal identification number (PIN). (FISCAM)

Term	Definition
Transaction	A discrete activity captured by a computer system, such as an entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records. (FISCAM)
Transaction File	*A group of one or more computerized records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods. (FISCAM)*
Trap Door	A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with back door. (NCSC-TG-004)
Trojan Horse	(1) A computer program that conceals harmful code. A **Trojan horse** usually masquerades as a useful program that a user would wish to execute. (FISCAM) (2) A destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful. (AISSP – Source: Microsoft Press Computer Dictionary)
Unauthorized Disclosure	Exposure of information to individuals not authorized to receive it. (NSTISSI)
Uncertainty	This term characterizes the degree, expressed as a percent, from 0.0 to 100%, to which there is less than complete confidence in the value of any element of the risk assessment. Uncertainty is typically measured inversely with respect to confidence, i.e., if confidence is low, uncertainty is high. (HISM)
Unclassified	Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (NSTISSI)

Term	Definition
UNIX	A multitasking operating system originally designed for scientific purposes which has subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. **UNIX** is also a major server operating system in the client/server environment. (FISCAM)
Update Access	This access level includes the ability to change data or a software program. (FISCAM)
User	(1) The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) (2) Any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (AISSP – Source: OMB Circular A-130)
User Identification (ID)	A unique identifier assigned to each authorized computer user. (FISCAM)
User Profile	A set of rules that describes the nature and extent of access to each resource that is available to each user. (FISCAM)
Utility Program	*Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery). (FISCAM)*
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (FISCAM)
Virus	(1) A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. (FISCAM) (2) A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. (NCSC-TG-004)

Term	Definition
Vulnerability	This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. Both expected frequency (ARO) and exposure factor (EF) for fire are increased as a consequence of not having a fire suppression system. (HISM)
WAN	See Wide Area Network.
Warning Banner	NIST Special Publication 800-12 Footnote 131: The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. The ambiguity results from the fact that current laws were written years before such concerns as keystroke monitoring or system intruders became prevalent. Additionally, no legal precedent has been set to determine whether keystroke monitoring is legal or illegal. System administrators conducting such monitoring might be subject to criminal and civil liabilities. The Department of Justice advises system administrators to protect themselves by giving notice to system users if keystroke monitoring is being conducted. Notice should include agency/organization policy statements, training on the subject, and a **banner** notice on each system being monitored. [NIST, CSL Bulletin, March 1993]
Wide Area Network (WAN)	(1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) (2) A communications network that connects geographically separated areas. (AISSP – Source: Microsoft Press Computer Dictionary)
Workstation	A microcomputer or terminal connected to a network. **Workstation** can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability. (FISCAM)

Term	Definition
Worm	(1) An independent computer Program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. (FISCAM) (2) A program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information. (AISSP – Source: Microsoft Press Computer Dictionary)
Write	Fundamental operation in an IS that results only in the flow of information from a subject to an object. (NSTISSI)
Write Access	Permission to write to an object in an IS. (NSTISSI)

References:

1. NCSC-TG-004 **–** Rainbow Series, Aqua Book, **Glossary of Computer Security Terms,** NCSC-TG-004-88, Library No. S-231, 238**.** Issued by the National Computer Security Center (NCSC).
2. FISCAM – Federal Information System Controls Audit Manual, GAO/AIMD-12.19.6
3. AISSP – Automated Information Systems Security Program Handbook, DHHS, http://wwworim.nih.gov/policy.assip.html, (for Source references see document)
4. Micki Krause and Harold F. Tipton, Handbook of Information Security Management (HISM), Imprint: Auerbach Publications, Publisher: CRC Press LLC, ISBN: 0849399475.
5. DoN **-** Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A, Aug. 3,1982. (Glossary)
6. NSTISSI – National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999 (Revision 1)
7. TechEncy – Technical Encyclopedia of definitions supported by TechWeb.com

GLOSSARY - The definitions in this glossary are drawn from several sources, including this manual, certain IBM manuals, and the documents and sources listed in the bibliography. In addition, certain definitions were developed by project staff and independent public accounting firms.

CMS
Core Set of Security Requirements

Attachment A

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

General Requirement Control Technique	Protocol	Reference

1. *Entitywide Security Program Planning and Management*

1.1 Management and staff shall receive security training, security awareness, and have security expertise.

1.1.1 Security training includes the following topics and the related procedures: (1) awareness training; (2) periodic security reminders; (3) user education concerning malicious software; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential).	1. Review training syllabus for inclusion of the required training. 2. Review a sample of training records to confirm completion of the required training. 3. Review documented procedure for generation of security reminders. 4. Review the training policy. 5. Interview a sample of site personnel to verify that documented training was received.	FISCAM HIPAA PDD 63

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

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

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

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

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

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

Guidance: Security awareness and security training should inform personnel, including contractors and other users of information systems that support Medicare claims processing of: (1) the proper rules of behavior while using Medicare claims processing systems and information, and (2) their responsibilities in complying with security policies and procedures. Security awareness and security training is provided before allowing access to any sensitive information or system. Security awareness should be a continuing effort but it should be repeated, minimally, on an annual basis. Related CSRs:

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

	General Requirement **Control Technique**	**Protocol**	**Reference**
1.1.4	Security training is adjusted or customized based on the level of the employee's role and responsibilities (i.e., the necessary security skills and competencies necessary to perform a specific role and responsibility).	For a sample of personnel, review training documentation and job descriptions for evidence of customization of security training to the level of job responsibilities.	CMS
	Guidance: Security training for an SSO or system security administrator requires more in-depth security skills and competencies (e.g., security controls, incident response, vulnerabilities, etc.) than a claims entry clerk who only requires basic security training on the proper use of security in relation to the processing of sensitive data (e.g., rules of behavior).	Related CSRs: 3.2.1, 3.2.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
1.1.5	The employees acknowledge, in writing, having received the security and awareness training.	1. Verify that records show all employees have acknowledged receiving security and awareness training. 2. Check a random sample of employees records to verify training attendance signature.	CMS FISCAM
	Guidance: No further guidance required.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
1.1.6	A record of the security awareness and security training subject(s) covered is maintained.	Verify that records are being maintained that document the security awareness and security training subjects covered.	CMS
	Guidance: There are several ways of maintaining these records. For example, the topics covered can be placed in an e-mail announcing the employees training and subsequently kept in a file.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
1.1.7	Training in emergency procedures is conducted at least once a year.	Verify the emergency procedures are dealt with in the COOP.	CMS
	Guidance: Emergency procedures should be defined in a procedure manual as part of the Contingency Plan and training performed annually. A record should be maintained that verifies that the training took place.	Related CSRs: 5.6.1, 5.6.3	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
1.1.8	Policy and security training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided.	Review documentation of policy and training to confirm the protection of copyright information under the terms of the provision of the copyright holder.	CMS
	Guidance: A security policy should exist, and security training should include, appropriate information regarding copyright protection.	Related CSRs: 3.3.1, 7.1.2, 10.7.2, 2.2.7	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
1.2	Management shall ensure that corrective security actions are effectively implemented.		
1.2.1	Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis.	1. Records providing information on the monitoring activities should be available. 2. Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested. 3. Review logs and policy documentation to verify that security corrective actions have been monitored on a continuing basis.	FISCAM HIPAA
	Guidance: A corrective security action would consist of designated safeguards from self-assessments, or similar items, developed as the result of an audit. Use of a designated manager, such as the SSO, to monitor implementation and to review the security configuration controls on a continuing basis would satisfy this requirement. This activity should be documented as an internal memorandum on an annual basis.	Related CSRs: 1.8.7, 1.12.3	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		

1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.

1.3.1 Business Partners transmitting (FTI) from a main frame computer to another computer, need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission. (This CSR applies only to the COB contractor.)

1. Review disclosure list for entries indicating that the documented process has been followed.
2. Interview responsible individual(s) to confirm understanding of the required procedure.
3. Review relevant policies and procedures for inclusion of the required logging process elements.
4. For a sample of documents being received from the IRS, observe handling of receipt of sensitive information for compliance with established procedures.

IRS 1075

Guidance: Transmission of FTI must be accompanied by appropriate records that will determine who released the information and what was released.

Related CSRs:

□ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

1.3.2 Sensitive information, other than that on magnetic tape files or disclosed as a function of normal claims processing operations (e.g., system processes, mailings, payments, etc.), disclosed outside the CMS Business Partner is recorded on a separate list that includes: (1) to whom the disclosure was made; (2) what was disclosed; (3) why it was disclosed; and (4) when it was disclosed.

1. Observe transmittal of sensitive information for compliance with established procedures.
2. Review relevant policies and procedures for inclusion of the required logging process elements.
3. Review disclosure list for entries indicating that the documented process has been followed.
4. Interview responsible individual(s) to confirm understanding of the required procedure.

HIPAA
IRS 1075

Guidance: This is a key element in controlling information within HIPAA. This needs to address areas such as e-mail and other means of transmission of sensitive information.

Related CSRs: 2.12.2

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

1.3.3 Appropriate controls are established for all sensitive data entering or leaving the facility. A system is employed that precludes erroneous or unauthorized transfer of data, regardless of media or format. Include controls that maintain a record for the logging of shipping and receipts and a periodic reconciliation of these records.

1. Evaluate the identified control procedures for inclusions of maintenance of records logging all shipping and receipts, and of periodic reconciliation of these records.
2. Review documented procedures for control of sensitive data entering or leaving the facility.
3. Evaluate the identified control procedures for inclusions of specific protections against erroneous or unauthorized transfers.
4. Review policy for relevance.

CMS
HIPAA

Guidance: Control procedures should be documented and defined in a Procedures Manual. Another approach would be to provide periodic training.

A policy and set of procedures should exist allowing for the establishment of records regarding sensitive information.

Related CSRs: 2.2.25, 2.2.26

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

1.3.4 A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.

1. Review the documented procedure for destruction of data.
2. Verify that the reviewed procedure includes protections against sensitive data becoming available to unauthorized personnel.

CMS

Guidance: A good concept is to establish a formal program with a policy and procedures for developing and maintaining records. A record should be maintained that verifies who performed the destruction and when sensitive information was destroyed.

Related CSRs: 1.3.5, 1.3.9

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

1.3.5 All retired, discarded, or unneeded sensitive data is disposed in a manner that prevents unauthorized persons from using it. All sensitive data is erased from storage media before releasing as work tapes or disks. Ensure the destruction of any sensitive information hard copy documents when no longer needed.

1. Review disposal procedures for inclusion of use of approved destruction methods during disposal of hard copy documents that are no longer needed.
2. For a sample of employees, interview to determine that disposal procedures are known and being followed.
3. Review disposal procedures for inclusion of use of approved sanitization procedures before release of any nonvolatile storage devices or media.
4. Review disposal procedures for inclusion of protections against use of retired, discarded, or unneeded sensitive data by unauthorized persons.

CMS
HIPAA
IRS 1075

Guidance: A good approach assures policies and procedures exist for release and/or destruction of CMS sensitive information.

Related CSRs: 1.3.4, 1.3.9

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

1.3.6 Sensitive data and CMS Business Partner records (Part A and Part B claims and benefit check records) are stored on-site. When on-site storage is not available, commercial storage facilities are used that most closely meet Federal standards for agency records centers. (Obtain Federal standards on National Archives Record Administration [36 CFR part 1228 subpart K]).

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. By inspection confirm that the specified data and records are stored on-site.

CMS

Guidance: When utilizing commercial storage facilities for off-site storage, ensure that any agreements in place address these Federal standards.

Related CSRs:

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

1.3.7 Sensitive information is never disclosed during disposal unless authorized by statute. Destruction of sensitive information is witnessed by a CMS Business Partner employee. However, a Business Partner may elect to have the destruction certified by a shredding contractor in the absence of Business Partner participation.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review a sample of destruction records to confirm consistent use of the procedure.

HIPAA
IRS 1075

Guidance: A formal program should be established with a policy and procedure. Review and update existing policy and procedures for addressing these requirements.

Related CSRs:

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

1.3.8 Before releasing files containing sensitive information to an individual or contractor not authorized to access sensitive information, care is taken to remove all such sensitive information. Procedures are in place to clear sensitive information and software from computers, memory areas, disks, and other equipment or media before they are disposed of or transferred to another use. The responsibility for clearing information is clearly assigned, and standard forms or a log is used to document that all discarded or transferred items are examined for sensitive information and this information is cleared before the items are released.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming consistent use of the required procedure.

FISCAM
HIPAA
IRS 1075

Guidance: It is good practice to review the media destruction procedures. In many cases, standard formatting will not remove sensitive data.
Additionally, a tracking or inventory system is used for the hardware but not the sensitive data residing in the electronic media. An approach to ensuring the sensitive data is cleared from the media is to test an reformat multiple times with an approved formatting technique.

Related CSRs: 2.12.2, 2.14.1

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

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

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming consistent use of the required procedure.

IRS 1075

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

Related CSRs: 1.3.4, 1.3.5

□ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

1.3.10 Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)

1. Confirm by inspection that facility has latest version of IRS Publication 1075.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review audit data confirming consistent use of the required receipt process.

IRS 1075

Guidance: It is a good approach when returning FTI information to CMS to obtain a receipt, and provide a notification which contains when and why the information was obtained, how long and for what reason(s) it was used, and when it was returned so as to make the FTI information usage traceable.

Related CSRs:

□ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

1.3.11 Destruction methods for sensitive information are as follows: (1) burning - the material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (2) mulching or pulping - all material is reduced to particles one inch or smaller; (3) shredding or disintegrating - paper is shredded in cross-cut shredders to a residue particle size not to exceed 1/32 inch in width (with a 1/64 inch tolerance) by 1/2 inch in length, and microfilm is shredded to 1/35 inch by 3/8 inch strips.

1. Review documentation confirming that destruction is accomplished using one or more of the approved methods.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

HIPAA
IRS 1075

Guidance: Destruction must be accomplished by burning, pulping, melting, chemical decomposition, mutilation, pulverizing, or shredding to the point of non recognition of the information. Ensure that a policy exists that describes, in detail, the procedures that employees must follow for the applicable method of destruction.

Related CSRs:

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

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

	General Requirement Control Technique	Protocol	Reference
1.3.12	Inventory records of all storage media containing sensitive data must be maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media will be recorded in a log that identifies: (1) date received, (2) reel/cartridge control number contents, (3) number of records if available, (4) movement, and (5) if disposed of, the date and method of destruction. Such a log must permit all storage media containing sensitive data (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and logged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming consistent use of the required procedure.	CMS FISCAM HIPAA IRS 1075 PDD 63
	Guidance: One method would be to ensure that deposits and withdrawals of tapes and other storage media from the library are authorized and logged and that audit trails kept as part of inventory management.	Related CSRs: 1.5.7	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc***	☑ ***DC***	☑ ***CWF***
1.3.13	Semiannual inventories of removable storage devices and media containing sensitive information are performed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.	IRS 1075 PDD 63
	Guidance: This approach helps to ensure that no removable storage devices or media are missing by performing and documenting a physical inventory twice a year.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc***	☑ ***DC***	☑ ***CWF***
1.3.14	Removable storage devices and media containing sensitive information are secured before, during, and after processing, and a proper acknowledgement form is signed and returned to the originator.	1. Review audit data confirming consistent use of the required procedure. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 PDD 63
	Guidance: A formal program should be established with a policy and procedure.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc***	☑ ***DC***	☑ ***CWF***
1.3.15	Whenever possible computer operations are in a secure area with restricted access. Sensitive information is kept locked when not in use. Tape reels, disks, or other media are labeled as CMS Sensitive Information. Media holding, processing or storing sensitive data is kept in a secure area.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming location of computer operations are in a secure area with restricted access, or that establishes approved use of equivalent safeguards.	CMS HIPAA IRS 1075 PDD 63
	Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information. When removing sensitive data tapes or other magnetic media from robotic systems, apply CMS sensitive information label(s).	Related CSRs: 2.2.16, 2.5.4	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc***	☑ ***DC***	☑ ***CWF***

1.4 Owners and users shall be aware of security policies.

1.4.1 Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; (6) assuring that system users, including maintenance personnel, receive security awareness training; and (7) implementing procedures to determine that the access of a workforce member to CMS sensitive information is appropriate.

1. Review a sample of training records to confirm completion of security awareness training.
2. Review training syllabus for inclusion of the security awareness training.
3. Review relevant policies and procedures for inclusion of the prescribed features.
4. Review personnel security records and job descriptions to verify that operating and maintenance personnel have the proper clearances.
5. Review access and maintenance logs, and interview a sample of operating and maintenance personnel, to verify that all maintenance access is logged, and that all maintenance is performed or supervised by authorized, knowledgeable personnel.

HIPAA

Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information.

Related CSRs: 4.2.2, 1.8.4, 2.2.19, 3.5.2, 5.9.9, 2.8.3, 2.8.5, 2.8.9

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

1.4.2 To provide reasonable assurance that sensitive information is adequately safeguarded, an annual self-assessment is conducted which addresses the safeguard requirements imposed by CMS. A copy of the self-assessment is submitted to CMS.

1. Review relevant policies and procedures for inclusion of the required self assessment process.
2. Review documentation confirming submittal of the most recent self assessment to CMS.

HIPAA
IRS 1075

Guidance: Annually complete the self assessment utilizing the Contractor Assessment Security Tool (CAST), and run the "Error Check Self-Assessments."

Related CSRs: 2.12.1, 1.8.6, 2.5.7, 2.5.8, 2.5.9

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

1.4.3 Reporting Improper Inspections or Disclosures of Sensitive Information - Upon discovery by any employee, the individual making the observation or receiving the information contacts his or her supervisor, who contacts CMS for submission to the appropriate authority.

1. Review relevant policies for inclusion of this directive.
2. For a sample of employees, interview to confirm familiarity with the policy and how to report such improper activity.

FISCAM
HIPAA
IRS 1075

Guidance: Establish procedures to identify apparent security violations and that suspicious activity is investigated and appropriate action taken.

Related CSRs:

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

1.4.4 Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; (3) rules that describe expected behavior of all with access to the system; and (4) procedures to prevent, detect, contain, and correct security violations.

1. Review policies and procedures for the required distribution process(es).
2. Review the distributed security policies for inclusion of the required rules.

FISCAM
HIPAA

Guidance: Establish procedures to distribute the security policies to all necessary personnel, and develop a process to document the receipt by the personnel.

Related CSRs: 6.4.1, 6.3.9, 9.6.1, 1.5.1

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

1.4.5 Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. The procedures: (1) stipulate what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.

Review relevant policies and procedures for inclusion and directed use of the required procedures.

CMS
HIPAA

Guidance: A good approach is to access the CERT WEB site for sample procedures for inclusion.

Related CSRs:

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

1.4.6 Medicare information is not used in the CMS Business Partner's private line of business unless authorized by CMS as consistent with the Privacy Act.

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

CMS

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

Related CSRs:

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

1.4.7 Employees are discouraged from browsing sensitive data files by making it clear that company policy prohibits it.

1. Interview a sample of employees to confirm awareness of, and adherence to this policy.
2. Review relevant policies for inclusion of the required directive.

CMS

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

Related CSRs:

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

1.5 Information security responsibilities shall be clearly assigned.

1.5.1 The system security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for: (1) information resource owners and users; (2) information resources management and data processing personnel; (3) senior management; and (4) security administrators.

1. Review the security plan for inclusion of the required identification of ownership of each computer-related resource, and of responsibilities for managing access to each of these resources.
2. Review the security plan for inclusion of definition of security responsibilities and expected behavior for at least each of the four specified categories of personnel.

FISCAM

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

Related CSRs: 1.4.4

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

1.5.2 The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.

Review documentation verifying that an SSO with the required qualifications is designated at an overall level, and at any subordinate levels designated as appropriate by the Business Partner.

CMS
FISCAM
HIPAA

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

Related CSRs: 9.6.3, 9.6.5, 9.6.6

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

1.5.3 If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.

1. If these additional SSO positions exist, review documentation supporting use of the specified process.
2. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.

CMS

Guidance: Ensure that all Medicare related actions are cleared through the primary Medicare SSO.

Related CSRs:

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

1.5.4 The SSO is organizationally independent of IS operations.

Review documentation supporting the required organizational independence.

CMS

Guidance: Ensure that the SSO's duties allow him/her to act independent of IS operations.

Related CSRs:

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

1.5.5 The SSO assures compliance with CMS's systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with CMS systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by CMS Regional Officer and/or Consortium; (4) ensuring that internal controls are incorporated into new ADP information systems; (5) ensuring that systems security requirements are included in RFPs and subcontracts involving Medicare claims processing; (6) maintaining systems security documentation for review by CMS Regional Officer and/or Consortium; (7) consulting with the CCMO's designated security officer on systems security issues when there is a need for guidance or interpretation; and (8) keeping up with new/advanced systems security technology; (9) is a member of all planning groups, having the responsibility to subject all new systems/installations (and major changes) to the risk assessment process; and (10) makes certain that specialists such as auditors, lawyers, and building engineers address security issues before changes are made.

1. Review documentation supporting SSO performance of each of the specified roles and responsibilities.
2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.

CMS
HIPAA

Guidance: An approach is to include these in the SSO's job description. Related CSRs: 9.6.3, 3.1.2, 1.9.4

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

1.5.6 The SSO in each CMS Business Partner organization is responsible for assisting Application System Managers in selecting and implementing appropriate administrative, physical, and technical safeguards for application systems under development or enhancement.

1. Review relevant documentation for designation of this security officer.
2. Review relevant policies and procedures for inclusion of identification of the specified roles and responsibilities of this security officer.

CMS

Guidance: An approach is to include these in the SSO's job description. Related CSRs: 6.3.13

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

1.5.7 Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.

Review documentation supporting designation of this responsibility to specific employees.

FISCAM
HIPAA
IRS 1075

Guidance: A good approach is to have the SSO designate specific employees this responsibility. Related CSRs: 1.3.12

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

1.6 An incident response capability shall be implemented.

1.6.1 Procedures exist to identify and report incidents: (1) security incident procedures; (2) report procedures; (3) response procedures; and (4) procedures to regularly review records of information system activity, such as security incident tracking reports.

1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.
2. Review security incident procedures

HIPAA

Guidance: Refer to sample procedures from the CERT WEB site. Related CSRs:

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

1.6.2 The CMS Business Partner's incident response capability has the following characteristics: (1) an understanding of the CMS Business Partners being served; (2) educated information owners and users that trust the incident handling team; (3) a means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; and (5) links to other relevant groups.

Review documentation supporting existence of the required characteristics within the Business Partner's incident response capability.

FISCAM

Guidance: Refer to sample procedures from the CERT WEB site. Related CSRs:

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

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

1.7.1 CMS has categorized sensitive Medicare data, FTI, and Privacy Act-protected data as sensitive information. These items are to be protected under the CMS Level 3 - High Sensitive security designation.

Protocol: Sensitive Information Safeguard Requirements verify that the combinations of protection implemented for Level 3 sensitive data match those specified in the Business Partner's System Security Manual, Section 4.3.

Reference: CMS
FISCAM
IRS 1075

Guidance: Ensure that a policy and procedure exist to categorize and protect all Medicare sensitive data as level 3 (See BPSSM).

Related CSRs: 2.5.2, 2.7.1, 2.2.7

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

1.8 Minimum protection standards shall consider local factors.

1.8.1 Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.

Protocol: Review relevant policies and procedures for inclusion of the required security management features.

Reference: HIPAA

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

Related CSRs: 3.1.2, 1.9.4

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

1.8.2 Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the system security plan.)

Protocol: Confirm by inspection that the required documentation is on file.

Reference: FISCAM
HIPAA

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

Related CSRs: 3.1.2

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

1.8.3 The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.

Protocol:

1. Review risk assessment policy for inclusion of the required factors.
2. Review the most recent high-level risk assessment for documentation of consideration of the required factors.

Reference: FISCAM
HIPAA

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

Related CSRs: 3.1.2, 2.7.1

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

1.8.4 A risk assessment is reviewed and updated annually or whenever significant modifications are made to a system, facility, or network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (policy, procedure, separating duties, security awareness and security training, testing/validating/editing, audit routines, audit trails/logs, alarms and fire extinguishing equipment, computer system automatic controls, manual controls, good housekeeping, secure disposal, authorizing/restricting access, relocating operations/equipment/records, modifying building/work environment, backup/encryption, insurance/bonding and maintenance/repair/replacement).

Protocol:

1. Review relevant policies and procedures for inclusion and directed use of the required process for determining the need for reassessment.
2. Review relevant policies and procedures for inclusion and directed use of the required content.
3. Review the most recent risk assessment for documented inclusion of the required content.

Reference: CMS
FISCAM
HIPAA
PDD 63

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

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

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

	General Requirement Control Technique	Protocol	Reference
1.8.5	Facilities housing sensitive and critical resources have been identified. All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	1. Review documentation supporting an assessment that all facilities housing sensitive and critical resources have been identified. 2. Review documentation supporting an assessment that all significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	FISCAM
	Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
1.8.6	A compliance review and self-assessment is conducted once a year.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming execution of the review process at least once a year.	CMS
	Guidance: Ensure that the CAST is completed once a year and that it is independently verified.	Related CSRs: 1.4.2, 2.5.7, 2.5.6	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
1.8.7	Top management initiates prompt actions to correct deficiencies.	1. Review documentation supporting consistent prompt action by top management to correct deficiencies. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM
	Guidance: An approach is to have senior management approve the corrective action plan and have quarterly updates to the plan.	Related CSRs: 1.2.1, 1.12.3	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
1.8.8	Major systems and applications are approved by the managers whose missions they support.	1. Inspect documentation of approval for each major system and application by the specified manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM
	Guidance: "Refer to the CMS SSPM for additional information guidance."	Related CSRs: 1.9.3	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
1.8.9	Local Information System risk factors are accessed in accordance with the CMS Information Security Risk Assessment (RA) Methodology and NIST SP 800-30.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying assessment of local risk factors in accordance with the reference.	CMS
	Guidance: This CSR should be addressed as part of a formal Risk Management Program.	Related CSRs: 1.9.8	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
1.8.10	Management analyzes local circumstances to determine space, container, and other security needs at individual facilities that meet or exceed the minimum protection requirements for the CMS Level 3 - High Sensitivity security designation.	Review documentation establishing that a location-specific Risk Analysis was conducted in development of each applicable System Security Plan.	CMS IRS 1075
	Guidance: See the Business Partners Security Manual for additional information and guidance.	Related CSRs: 2.2.11, 2.2.9	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

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

1.9.1 The following are accomplished and documented: (1) security configuration documentation; (2) hardware/software installation and maintenance review and testing for security features; (3) inventory records; (4) security testing; and (5) checking for malicious software.

1. Review the security plan for inclusion of the required elements.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation supporting completion of the required security testing.

HIPAA

Guidance: Policies and Procedures should exist that address these 5 items.

Related CSRs: 5.9.3, 5.12.1, 2.5.1

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

1.9.2 Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.

Review relevant policies and procedures for inclusion and directed use of the required process.

HIPAA

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Related CSRs:

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

1.9.3 A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties and covers the topics prescribed by OMB Circular A-130 such as: (a) rules of the system/application rules; (b) security awareness and security training; (c) personnel controls/personnel security; (d) incident response capability; (e) continuity of support/contingency planning; (f) technical security/technical controls; (g) system interconnection/information sharing; (h) public access controls.

1. Review documentation verifying that a security plan covers all major facilities and operations.
2. Review documentation verifying that the security plan has been approved by all key affected parties.
3. Inspect the security plan to confirm that it covers all of the specified topics.

FISCAM
HIPAA

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Related CSRs: 1.8.8, 6.1.2, 6.3.4, 10.7.3

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

1.9.4 A system security plan has been prepared, in accordance with the CMS SSP Methodology, to cover every application and system categorized as a Major Application (MA) or General Support System (GSS).

1. Review documentation establishing that preparation of the plan was in accordance with the CMS SSP Methodology.
2. Review documentation verifying coverage by system security plans for all applications categorized as MA and GSS.

CMS

Guidance: Refer to the CMS System Security Plans Methodology for further guidance.

Related CSRs: 9.4.1, 3.2.4, 3.3.2, 3.4.6, 3.5.2, 3.5.3, 3.5.6, 3.6.2, 3.6.3, 1.8.1, 1.5.5

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

1.9.5 The CMS Business Partner System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self-assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, CMS, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10) authorization lists that include the designation of the individual responsible for handling security violations and each individual (or position title) responsible for individual assets; and (11) lists of other security records such as audit trails/logs and visitor sign-in sheets. Include all other CMS directed or Business Partners System Security Manual directed documents.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.

CMS
HIPAA

Guidance: One method is to incorporate these requirements into the SSO's job description.

Related CSRs: 3.3.4, 2.2.17, 2.2.19

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

1.9.6 Retention procedures are established for all CMS sensitive information.

Protocol: Review documents establishing the appropriate retention procedures.

Reference: CMS
HIPAA

Guidance: Review retention procedures in relation to CMS PMs.

Related CSRs:

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

1.9.7 Documentation is available to assure that the level of sensitivity and criticality designations of each system has been assigned and has been determined to be commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.

Protocol: Review documentation establishing that the required designations have been assigned with the considerations specified.

Reference: CMS

Guidance: Review the BPSSM and apply risk mitigation controls.

Related CSRs: 3.1.2

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

1.9.8 Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.

Protocol:

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data verifying that vulnerability identification has been performed as specified.
3. Establish by inspection that the required summary lists are available.

Reference: PDD 63

Guidance: Review risk assessment.

Related CSRs: 1.8.9, 10.9.4

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

1.9.9 The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.

Protocol:

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data supporting conduct of the required periodic reviews.
3. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.

Reference: FISCAM

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Related CSRs:

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

1.9.10 The system security plan establishes a security management structure with adequate independence, authority and expertise.

Protocol:

1. Verify by inspection that the system security plan contains the required management structure.
2. Review documentation supporting the assertion that the security management structure meets the stated requirements.

Reference: FISCAM

Guidance: Refer to the CMS System Security Plan Methodology for further guidance.

Related CSRs:

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

1.10 Security policies shall exist that address hiring, transfer, termination, and performance.

1.10.1 For prospective employees, references are contacted and background checks performed.

Protocol:

1. Inspect personnel records to confirm that references have been contacted and background checks have been performed.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

Reference: CMS
FISCAM

Guidance: As part of the HR function, develop a policy and procedure to address hiring, transfer, termination, and performance items.

Related CSRs:

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

1.10.2 Regular job or shift rotations are required for those personnel using sensitive information.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review staff assignment records to confirm that job and shift rotations occur.

FISCAM

Guidance: Personnel whose duties or position gives them access to input or modify sensitive data in such a manner that fraud may be committed should be periodically rotated into different jobs or different shift rotations to introduce other personnel into the process. These rotations increase the likelihood that collaborative fraudulent activities by multiple employees will be disrupted and identified.

Related CSRs:

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

1.10.3 Regularly scheduled vacations exceeding several days are required for those personnel using sensitive information.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of personnel records to confirm compliance with the required vacation policy.

FISCAM

Guidance: An approach is a policy developed that requires employees using sensitive information to take a minimum of 24 hrs continuous vacation.

Related CSRs:

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

1.10.4 Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.

1. Review termination and transfer procedures for inclusion of the required processes.
2. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
3. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.

FISCAM
HIPAA

Guidance: These items need to be addressed as part of a HR Termination/Transfer procedure.

Related CSRs: 2.9.9, 2.2.20, 2.8.1

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

1.10.5 Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.

1. Review documentation establishing that reinvestigation policies for each position are consistent with the specified criteria.
2. Inspect personnel records to confirm sensitive position have had background reinvestigations performed within the required period.

FISCAM

Guidance: CMS will provide future direction.

Related CSRs: 2.5.5

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

1.10.6 Confidentiality or security agreements are required for CMS Business Partner Medicare employees and their contractors assigned to work with sensitive information.

1. Review policies on confidentiality or security agreements.
2. Determine whether confidentiality or security agreements are on file.
3. Review a sampling of agreements.

FISCAM
HIPAA

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

Related CSRs:

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

1.11 Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.

1.11.1 Disclosure of sensitive information is prohibited unless specifically authorized by statute.

1. Review Authorized Disclosure Agreements.
2. Review relevant policies for inclusion and directed use of the required directive.

CMS
IRS 1075

Guidance: The HIPAA privacy rules should be reviewed.

Related CSRs:

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

1.11.2 Written contracts or other arrangements require the inclusion of the CMS Core Security Requirements to protect the integrity, confidentiality, and availability of the electronically exchanged data. The CMS Business Partner will maintain a list of all contracts or other arrangements with other CMS Business Partners or business associates (include organization name and location, contract or agreement number, and purpose). The list of contracts will be provided to CMS in an MS Word document with the annual CAST submission.

1. Review documented arrangements/contracts for security content.
2. Verify risk-based decision is justified.

CMS
HIPAA

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

Related CSRs:

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

1.11.3 The CMS Business Partner has obtained satisfactory assurances that all external business associates will provide appropriate safeguards for CMS sensitive information.

1. Review the implemented safeguards.
2. Ensure satisfactory assurances have been provided.

HIPAA

Guidance: A good approach may be to provide a risk-based solution. All contracts should be part of the security profile and available to the SSO for review.

Related CSRs:

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

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

1.12.1 The System Owner/Manager, System Maintainer, or Senior Management designee signs the SSP and certification package.

Inspect the SSP and certification package for the required signatures.

CMS

Guidance: Review SSP certification package.

Related CSRs:

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

1.12.2 The safeguard selection decisions and the risk assessment reports submitted are carefully reviewed.

Examine documentation supporting completion of the required review.

CMS

Guidance: Review risk assessment for mitigation of risks and provide recommendations.

Related CSRs:

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

1.12.3 The CMS Business Partner is responsible for approving any necessary corrective action plans.

1. Review audit data supporting compliance with the required approval process.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. A plan of action is documented for correcting security deficiencies.

CMS

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

Related CSRs: 1.8.7, 1.2.1

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

1.12.4 The CMS Business Partner's systems security certification is completed annually and is fully documented.

1. Review documentation confirming that the last CMS Business Partner's systems security certification or recertification was completed within the last year.
2. Review documentation supporting an assertion that the security system is fully documented.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

CMS

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

Related CSRs:

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

1.13 General workstation security requirements shall be established.

1.13.1 Policies and procedures are implemented that specify the proper workstation functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access CMS sensitive information.

1. Verify by inspection that the required policy/guideline is available.
2. Interview a sample to confirm familiarity with the required document.

HIPAA

Guidance: One approach would be to address all the local workstations as well as the workstations used at home.

Related CSRs: 7.3.3, 7.3.4, 7.3.5, 7.4.1, 7.4.2, 7.5.1

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

1.13.2 Policy states that employees are not permitted to bring their personally owned computers into the workplace.

Review the specified policy.

CMS

Guidance: Bringing personal computers into the workplace creates vulnerabilities to the Medicare resources and compromises sensitive data.

Related CSRs:

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

1.13.3 All CMS-owned software (such as CAST) is secured at close of business or anytime that it is not in use. Manuals and diskettes or CD-ROMs are stored out of sight in desks or file cabinets.

1. Interview programmers and system manager.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review audit data confirming enforcement of the required process.

CMS

Guidance: No further guidance required.

Related CSRs: 10.7.1

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

1.13.4 If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation describing the process used to assure compliance with the required policy.

CMS

Guidance: An approach is to establish policies and procedures that address working "off-site." These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.

Related CSRs: 2.2.27

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

1.13.5 Policies are established for controlling the use of laptops, notebooks and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.

Determine the effectiveness of controlling portable terminals by review business partner mobile computing policies.

CMS

Guidance: An approach is to establish policies and procedures that address working "off-site." These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.

Related CSRs: 2.2.27

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

2. *Access Control*

2.1 Audit trails/logs shall be maintained.

2.1.1 User account activity audits are conducted using automated audit controls.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation describing the automated controls installed to implement the required process.
3. Inspect activity audit logs to confirm continuing use of the required process.

HIPAA

Guidance: Automated tools support real-time and after-the-fact monitoring. They assist in identifying questionable data access activities, investigating breaches, responding to potential weaknesses, and assessing the security program. Audit reduction tools and/or “intelligent” methods of correlating log data may be used to detect unauthorized activity and reduce volumes to manageable size.

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

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

2.1.2 Computer systems processing sensitive information are secured from unauthorized access. All security features are available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing sensitive information is accountable.

1. Review documentation identifying all security features of each hardware and software item in the system, and the extent to which each feature is available and activated.
2. Review documentation establishing that the computer systems processing sensitive information are secured from unauthorized access.
3. For a sample of hardware and software security features, obtain demonstrations of feature operation.
4. Review documentation describing how audit facilities are utilized to assure that everyone accessing a computer system containing sensitive information is accountable.

HIPAA
IRS 1075

Guidance: Safeguards are in place to eliminate or minimize the possibility of unauthorized access to sensitive information.

The computer systems identified should include those that process Standard Systems, clients used by claims processors, and related computers with sensitive information such as e-mail.

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

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

	Control Technique	Protocol	Reference
2.1.3	All activity involving access to and modifications of sensitive or critical files is logged.	1. Validate the types of files involved and the features are turned on or coding has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation describing how compliance with this requirement is assured. This should include documentation specifically designating all files considered sensitive or critical, with identification of the corresponding logging methodology for each of these files. 4. Inspect samples of the specified audit logs to confirm continuing use of the required process.	FISCAM

Guidance: Access control software is used to maintain an audit trail of security accesses to determine how, when, and by whom specific actions were taken.

In general, the database systems and some transaction systems support this feature. When the critical files are flat files, the feature will require some additional coding.

Related CSRs: 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

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

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

Guidance: Computer security managers and system administrators or managers should have read-only access for review purposes; however, security and/or administration personnel who maintain logical access functions should not have access to audit logs.

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

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

	Control Technique	Protocol	Reference
2.1.5	The audit trail includes sufficient information to establish what events occurred and who or what caused them.	1. Review a sample of event logs and audit records to confirm the required content. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS

Guidance: In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result. Date and time can help determine if the user was a intruder or the actual person specified.

Related CSRs: 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

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

2.1.6 Audit trails/logs are reviewed periodically (i.e., minimum of weekly) and retained for a minimum of 60 days.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of audit data confirming that audit logs are being retained for the same period as the related claim.
3. Inspect a sample of audit data confirming that the required reviews have been conducted.

CMS
HIPAA

Guidance: Maintain, and periodically review, audit logs for critical application systems, including user-written applications. Audit logs may become evidence in legal proceedings, so care should be taken to protect their integrity

Related CSRs: 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5

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

2.1.7 All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.

1. Inspect device configurations to confirm that all detected errors that can be logged are being logged.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Determine that audit logs have sufficient detail to assist with fault isolation and resolution of security abnormalities.

CMS

Guidance: Audit trail analysis can often distinguish between operator-induced errors (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code). If a system fails or the integrity of a file (either program or data) is questioned, an analysis of the audit trail can reconstruct the series of steps taken by the system, the users, and the application. If a technical problem occurs (e.g., the corruption of a data file) audit trails can aid in the recovery process (e.g., by using the record of changes made to reconstruct the file). Correct confirmation of hardware fault routines will provide better recovery techniques and the recorded information will provide better results from hardware maintenance engineers.

Related CSRs:

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.

2.2.1 Physical Intrusion Detection Systems (IDS) are used to provide the security of sensitive information in conjunction with other measures that provide forced entry protection during non-working hours. Alarms annunciate at an on-site protection console, a central station, or local police station. IDS include, but are not limited to: (1) door and window contacts; (2) magnetic switches; (3) motion detectors; and (4) sound detectors.

1. Review physical intrusion detection policies and procedures for spaces and rooms containing sensitive information for inclusion of the specified approach.
2. Review documentation describing measures used in conjunction with IDS to enhance protections provided directly by the IDS.

FISCAM
IRS 1075

Guidance: Physical security controls used to detect access to facilities and protect them from intentional and unintentional loss or impairment.

Related CSRs: 3.6.5

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

Category: *Access Control*

	General Requirement Control Technique	Protocol	Reference
2.2.2	Restricted areas are prominently posted and separated from non-restricted areas by physical barriers that control access. All entrances have controlled access (e.g., electronic access control, key access, door monitor) and the main entrance to restricted areas is manned.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required controls. 3. Inspect restricted area access points to confirm that the documented controls are in place and operational.	CMS IRS 1075
	Guidance: A restricted area is an area where entry is restricted to authorized personnel. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information. Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a LAN server. The controls can include controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points.	Related CSRs: 2.8.6, 5.2.7	
	☑ SS ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF		
2.2.3	All restricted areas used to protect sensitive information meet CMS criteria for secured area or security room, or provisions are made to store CMS sensitive information in appropriate security containers during non-working hours.	If Restricted Areas are used to protect sensitive information, review documentation establishing that each meets the specific CMS requirements for either a "Secured Area" or a "Security Room", or that provisions have been made to store CMS sensitive information in appropriate security containers during non-working hours.	CMS IRS 1075
	Guidance: Review BPSSM Section 4 for guidance.	Related CSRs:	
	☑ SS ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF		
2.2.4	Secured areas/perimeters designed to prevent undetected entry by unauthorized persons during non-working hours are: (1) enclosed by slab-to-slab walls, constructed of approved materials, and supplemented by periodic inspection or other approved protection methods; (2) Any lesser-type partition is supplemented by UL approved electronic intrusion detection and fire detection systems; (3) Unless intrusion detection devices are used, all doors entering the space are locked and strict key or combination control is exercised. In the case of a fence and gate, the fence has intrusion detection devices or is continually guarded and the gate is either guarded or locked with intrusion alarms; and (4) The space is cleaned during working hours in the presence of a regularly assigned employee.	1. Review documentation confirming that secured area/perimeters have the required features. 2. Inspect a sample of audit data confirming that the space is cleaned during working hours in the presence of a regularly assigned employee. 3. Inspect a sample of audit data confirming that the secured area/perimeters are consistently secured at the end of working hours, and found secured when opened for business. 4. Confirm by inspection that the required electronic intrusion devices are in use.	CMS IRS 1075
	Guidance: The controls over physical access to the elements of a system can include restricted or controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points. Walls forming secured areas should be slab-to-slab or true floor to true ceiling. They should be constructed of substantial materials such as masonry or heavy plywood to prevent the spread of fire and surreptitious entry. The interior walls can be constructed of drywall or plaster board partitions. Review BPSSM Section 4.	Related CSRs: 2.2.5	
	☑ SS ☑ PartB ☑ PartA ☑ Dmerc ☑ DC ☑ CWF		

	General Requirement Control Technique	Protocol	Reference
2.2.5	Security rooms include the following features: (1) entire room is enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection; (2) all doors entering the space are locked with approved locking systems; (3) any glass in doors or walls is security glass (a minimum of two layers of 1/8-inch plate glass with .060-inch [1/32] vinyl interlayer, nominal thickness is 5/16-inch); (4) plastic glazing material is not acceptable; (5) vents and/or louvers are protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station, and is given top priority for guard/police response during any alarm situation; and (6) cleaning and maintenance is performed in the presence of an employee authorized to enter the room.	If Security Rooms are used, review documentation confirming that each includes all of the required features.	CMS IRS 1075
	Guidance: The purpose of security rooms is to store protectable material. Walls forming the perimeter of security rooms should be slab-to-slab or true floor to true ceiling. They should be constructed of substantial materials such as masonry or heavy plywood to prevent the spread of fire and surreptitious entry. The interior walls can be constructed of drywall or plaster board partitions. If security rooms are used, review the requirements in BPSSM Section 4.	Related CSRs: 2.2.4	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.2.6	Locking Systems for Secured Areas and Security Rooms - High-security pin-tumbler cylinder locks are used that meet the following requirements: (1) key-oriented mortised or rim-mounted deadlock bolt; (2) dead bolt throw of one inch or longer; (3) double-cylinder design; (4) cylinders have five or more pin tumblers; (5) if bolt is visible when locked, it contains hardened inserts or is made of steel; and (6) both the key and the lock are "Off Master." Convenience-type locking devices (e.g., card keys, sequence button-activated locks, etc.) used in conjuction with electric strikes are authorized for use during working hours only. Keys to secured areas are never in personal custody of an unauthorized employee and combinations are stored in a security container.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.	CMS IRS 1075
	Guidance: Security rooms are constructed to resist forced entry and their primary purpose is to store protectable material. Secured areas are interior areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours. The minimum requirements for their locking systems, as stated in this requirement, is contained in BPSSM Section 4. (Also refer to BPSSM Section 4 for additional information on security rooms and secured areas.)	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.2.7	Sensitive information in any form is protected during non-working hours through a combination of a secured or locked perimeter, a secured area, or appropriate containerization.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used. 3. Review documentation establishing the protective methods and devices employed to protect sensitive information during non-working hours. Confirm use of one or more of the following controls: (1) secured or locked perimeter; (2) secured area; or (3) containerization.	CMS IRS 1075
	Guidance: Review BPSSM Section 4 for guidance.	Related CSRs: 1.1.8, 1.7.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.2.8	Sensitive information (including tapes or cartridges) are placed in secure storage in a secure location, safe from unauthorized access. All containers, rooms, buildings, and facilities containing sensitive information are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.	1. Review facility security plan for procedures and policies for protection of sensitive information. 2. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of sensitive information data.	CMS IRS 1075
	Guidance: Media controls should be planned for and designed to prevent the loss of confidentiality, integrity, or availability of sensitive information, including data or software, when stored outside the system.	Related CSRs: 6.4.2	
	☑ *SS* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF*		
2.2.9	Sensitive information outside secured areas or security rooms during non-working hours is stored in one of the following: (1) metal lateral key lock files; (2) metal lateral files equipped with lock bars on both sides and secured with security padlocks; (3) metal pull-drawer cabinets with center or off-center lock bars secured by security padlocks; or (4) key lock "mini safes" properly mounted with appropriate key control.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements. 3. Review documentation supporting the contention that the required process is followed for storage of sensitive information.	CMS IRS 1075
	Guidance: Sensitive information kept within secured areas or security rooms during non-working hours can be stored in locked containers and do not require a security container. Otherwise, sensitive information must be stored in a security containter or safe/vault. (See BPSSM Section 4 for additional information concerning these terms and requirements.)	Related CSRs: 1.8.10	
	☑ *SS* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF*		
2.2.10	If safes and/or vaults are used, they comply with: (1) A safe is a GSA-approved container of Class I, IV, and V, or Underwriters Laboratories (UL) listings of TRTL-30, TXTL-60, or TRTL-60; (2) A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, and uses UL-approved vault doors, and meets GSA specifications.	Examine safe(s) or vault(s) for accompanying manufacturer documentation.	CMS IRS 1075
	Guidance: Safes and/or vaults are not required for storage of sensitive information if provisions have been made to store CMS sensitive information in other appropriate security containers. However, if they are used, they must meet these GSA/UL requirements as stated in BPSSM Section 4.	Related CSRs:	
	☑ *SS* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF*		
2.2.11	Locked containers must include lock mechanisms that use either a built-in key, or hasp and lock, and include the following features: (1) metal cabinet or box with riveted or welded seams, or (2) metal desks with locking drawers.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of containers to confirm inclusion of the required features.	CMS IRS 1075
	Guidance: A locked container is any metal container which is locked and to which keys and combinations are controlled.	Related CSRs: 1.8.10	
	☑ *SS* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF*		
2.2.12	Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.	Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.	HIPAA
	Guidance: Workstations are located in controlled access areas and are safeguarded from unauthorized access.	Related CSRs: 2.8.6, 3.6.3, 7.3.3, 7.3.7	
	☑ *SS* ☑ *PartB* ☑ *PartA* ☑ *Dmerc* ☑ *DC* ☑ *CWF*		

	General Requirement Control Technique	Protocol	Reference
2.2.13	Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.	1. If methods used to deny access to sensitive information by unauthorized personnel during working hours do not include use of Restricted Areas, Security Rooms, or Locked Rooms, then review documentation justifying use of alternative methods. 2. Review documentation establishing the methods employed to deny access to sensitive information from unauthorized personnel during working hours.	HIPAA IRS 1075
	Guidance: Procedures for limiting physical access ensure that properly authorized access is allowed.	Related CSRs: 2.5.1, 2.5.3	
	☑ *SS* ☑ *PartB* ☑ *PartA*	☑ *Dmerc* ☑ *DC*	☑ *CWF*
2.2.14	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter restricted and other security areas after fire drills or other evacuation procedures.	1. Review written emergency procedures for inclusion of the required process. 2. Inspect a sample of audit data confirming use of the required process.	FISCAM
	Guidance: Re-entry access methods are used to provide appropriate controls at emergency exits.	Related CSRs: 5.6.2, 2.8.8	
	☑ *SS* ☑ *PartB* ☑ *PartA*	☑ *Dmerc* ☑ *DC*	☑ *CWF*
2.2.15	Procedures exist for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that the required process is consistently used.	HIPAA
	Guidance: Policies and procedures for limiting physical access ensure that properly authorized access is allowed.	Related CSRs: 2.4.2, 2.8.9, 2.8.3	
	☑ *SS* ☑ *PartB* ☑ *PartA*	☑ *Dmerc* ☑ *DC*	☑ *CWF*
2.2.16	Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	1. Review documentation designating specific individuals who are allowed access, and identifying the associated access control method used. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review a sample of audit data confirming consistent use of the required access process.	FISCAM PDD 63
	Guidance: Through the use of security controls, limit access to personnel with a legitimate need for access to perform their duties.	Related CSRs: 1.3.15, 2.1.2, 2.5.4, 9.2.1, 2.9.4	
	☑ *SS* ☑ *PartB* ☑ *PartA*	☑ *Dmerc* ☑ *DC*	☑ *CWF*

	General Requirement Control Technique	Protocol	Reference
2.2.17	Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of sign-in/sign-out registers to confirm collection of the required information. 3. Review a sample of audit data confirming compliance with the required register close out and review actions 4. Inspect a sample of audit data confirming monthly issue of a new AAL.	FISCAM HIPAA IRS 1075

Guidance: Persons other than regular authorized personnel may be granted access to sensitive areas or facilities, but these visitors are controlled and not granted unrestricted access.

Related CSRs: 1.9.5, 2.6.3

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

2.2.18	Management regularly reviews the list of persons with physical access to sensitive facilities.	1. Review a sample of audit data confirming periodic completion of the required reviews. 2. Review relevant policies and procedures for inclusion and directed use of the required process, and that they specify the review period.	FISCAM HIPAA

Guidance: Access to sensitive facilities should be limited to personnel with a legitimate need for access to perform their duties.

Related CSRs: 2.8.5

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

2.2.19	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	1. Review audit data confirming consistent use of the required procedure. 2. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.	FISCAM

Guidance: Access should be limited to personnel with a legitimate need for access to perform their duties, and they should be controlled and not be granted unrestricted access.

Related CSRs: 1.4.1, 1.8.4, 1.9.5

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

2.2.20	Key combinations are changed when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.	1. Review audit data confirming consistent use of the required process. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	HIPAA IRS 1075

Guidance: There are procedures for revoking physical access to controlled areas and removing user accounts when employees terminate employment or when others, such as contractors and vendors, no longer require access.

Related CSRs: 1.10.4, 2.9.9, 2.8.1

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

2.2.21	All entry code combinations are changed periodically.	1. Review documentation and logs for entry code changes. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM

Guidance: Periodically changing entry codes prevents reentry by previous employees or visitors who might have knowledge of the entry code.

Related CSRs:

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.2.22	Unissued keys or other entry devices are secured.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.	FISCAM
	Guidance: Unissued keys and other entry devices should be stored in appropriate security containers.	Related CSRs:	
		☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	
2.2.23	Keys or other access devices are needed to enter the computer room and tape/media library.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming implementation and use of the required control.	FISCAM HIPAA
	Guidance: Access to these areas should be limited to personnel with a legitimate need for access to perform their duties.	Related CSRs: 2.8.6, 10.1.1	
		☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	
2.2.24	Transmission and Storage of Data - Sensitive information may only be stored on hard disk as long as the CMS Business Partner approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades and are being used. Access control devices include: (1) password security; (2) audit trails/logs; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documentation of approval and installation of the required devices. 3. Review documentation confirming that the access control devices include the required features. 4. Review audit data confirming accomplishment of the required maintenance and upgrades, 5. Review audit data confirming consistent use of the required control devices.	CMS IRS 1075
	Guidance: The methodology used to ensure confidentiality, both in storage and transmission, can be software based, hardware based, or a combination of both. The robustness of protection provided shall be commensurate with the sensitivity of the information.	Related CSRs: 5.9.6, 5.12.1, 3.6.1	
		☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	
2.2.25	Handling and Transporting Bulk Sensitive Information - Care is taken to safeguard sensitive information at all times. If hand carried between facilities, it is kept with an individual and protected from unauthorized disclosure. All shipments between facilities are documented on transmittal forms and monitored. All bulk shipments transmitted by the U.S. Postal Service, common carrier, or messenger service shall be sent in a sealed, opaque envelope, addressed by name and organization symbol, and marked "To be opened by addressee only."	1. Review sensitive information handling and transporting policies and procedures for control technique compliance. 2. Review sensitive information transmittal forms for accuracy and completeness. 3. Inspect a sample of sensitive information data media for labeling compliance with the requirement.	CMS
	Guidance: These procedures apply for the routine and non-routine receipt, handling, and transporting of sensitive information between facilities, and are documented. However, these procedures are not meant to apply to routine claims handling and mailings between the carrier and Medicare recipients.	Related CSRs: 1.3.3, 2.5.4	
		☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	

2.2.26 Sensitive information is locked in cabinets or sealed in packing cartons while in transit. Sensitive information material remains in the custody of a CMS or CMS Business Partner employee. Accountability is maintained during the move.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of audit data supporting continuing use of the required processes.

HIPAA
IRS 1075

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

Related CSRs: 1.3.3

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

2.2.27 Alternate work site equipment controls are: (1) only CMS Business Partner-owned computers and software are used to process, access, and store sensitive information; (2) specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with their managers or other members of the Business Partner security staff in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller, Business Partner-owned equipment is locked in a storage cabinet or desk when not in use.

1. Review relevant policies and procedures for inclusion and directed use of the required process by personnel working from their homes or alternate worksites.
2. Inspect documentation confirming that the required controls are implemented and consistently used.

CMS
IRS 1075

Guidance: Employees processing sensitive information at alternate work sites (e.g., home, other contractor or facility) must satisfy these equipment controls to properly protect sensitive information.

An alternate work site is not a hotsite. Alternate work sites are those areas where employees, subcontractors, consultants, auditors, etc. perform work associated duties. The most common alternate work site is an employee's home. However, there may be other alternate work sites such as training centers, specialized work areas, processing centers, etc.

Related CSRs: 1.13.4, 1.13.5

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

2.2.28 Responsibility is assigned and security procedures are documented for bringing hardware and software into and out of the facility, as well as movement of these items within the facility, and for maintaining a record of those items.

Inspect documentation confirming that the required controls are implemented and consistently used.

HIPAA

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

Related CSRs:

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

2.2.29 Procedures are implemented to control access to software programs undergoing testing or revision.

Procedures are in place to protect CMS sensitive information during software testing and revisions.

HIPAA

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

Related CSRs:

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

2.2.30 Policies and procedures are implemented to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).

A maintenance tracking system should be implemented.

HIPAA

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

Related CSRs:

□ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

2.3 Access paths shall be identified.

2.3.1 An analysis of the logical access paths is performed whenever changes to the system are made.

1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM

Guidance: It is important that all access paths (e.g., Internet, dial-in, telecommunications) be identified and controlled to eliminate "backdoor" paths.

Related CSRs: 3.4.1, 4.5.1

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

2.4 Emergency and temporary access authorization shall be controlled.

2.4.1 Procedures are established (and implemented as needed) that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

1. Review documentation of the access control process to confirm inclusion of a procedure for emergency access.
2. Review documentation of the access control process to confirm inclusion of at least one of the required features.

HIPAA

Guidance: The mechanism is used to control emergency and temporary access authorizations. Emergency access typically requires unsupervised changes and should require verification and review as part of the procedures.

Related CSRs: 5.2.7, 5.6.2, 2.9.12

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

2.4.2 Emergency and temporary access authorizations are: (1) documented on standard forms and maintained on file; (2) approved by appropriate managers; (3) securely communicated to the security function and; (4) automatically terminated after a predetermined period.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of audit data confirming that all four specified elements of the required process is consistently used.

FISCAM

Guidance: As with normal access authorizations, emergency and temporary access should be approved and documented.

Related CSRs: 5.2.7, 2.2.15, 2.8.3, 2.8.9

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

2.5 Resource classifications and related criteria shall be established.

2.5.1 To meet functional and assurance requirements, the operating security features of sensitive information systems must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to sensitive information.

1. Inspect documentation identifying systems that process sensitive information.
2. Review documentation establishing that all computers in all specified systems meet requirements in their implemented configuration.
3. Review documentation of the configuration management process used to assure that all systems remain in certified configurations.

CMS
IRS 1075

Guidance: The purpose of security is to support the function of the system, not to undermine it. Therefore, many aspects of the function of the system will produce related security requirements. Assurance documentation can address the security either for a system or for specific components. System-level documentation should describe the system's security requirements and how they have been implemented, including interrelationships among applications, the operating system, or networks. System-level documentation addresses more than just the operating system, the security system, and applications; it describes the system as integrated and implemented in a particular environment. Component documentation will generally be an off-the-shelf product, whereas the system designer or implementor will generally develop system documentation.

Related CSRs: 2.2.13, 1.9.1, 2.1.2

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

2.5.2 Classifications and criteria have been established and communicated to resource owners.

1. Review policies specifying classification categories and related criteria to be used by resource owners in classifying their resources according to the need for protective controls.
2. Inspect audit data confirming that the required policy has been communicated to resource owners.

FISCAM

Guidance: Policies and procedures specifying classification categories and related criteria are established in accordance with Section 4 of the BPSSM to help resource owners classify their resources according to their need for protection controls.

Related CSRs: 1.7.1, 2.7.1

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.5.3	Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation establishing that existing safeguards provide the required protections.	HIPAA IRS 1075 PDD 63
	Guidance: Policies and procedures limit access while ensuring that properly authorized access is allowed based on an employee's need-to-know.	Related CSRs: 2.12.1, 2.2.13, 2.7.2, 2.9.4	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.5.4	Sensitive information is kept separate from other information to the maximum extent possible. Files are clearly labeled to indicate that sensitive information is included. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information.	1. Review sensitive information handling procedures for inclusion of the required processes. 2. For a sample of media and devices containing sensitive information, inspect to confirm use of the required labels.	CMS IRS 1075
	Guidance: Controlling media may require some form of physical labeling. The labels can be used to identify media with special handling instructions, to locate needed information, or to log media (e.g., with serial/control numbers or bar codes) to support accountability. Identification is often by labels on diskettes or tapes or banner pages on printouts.	Related CSRs: 2.2.16, 1.3.15, 2.2.25	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.5.5	Every personnel position with access to CMS sensitive information processing is designated with a sensitivity level, and documentation is available to support the security and suitability standards for these personnel commensurate with their position sensitivity level and appropriate personnel investigation requirements.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample of personnel positions, inspect documentation establishing the associated sensitivity level.	CMS PDD 63
	Guidance: The staffing process generally involves: (1) defining the job, normally involving the development of a position description; (2) determining the sensitivity level of the position; (3) filling the position, which involves screening applicants and selecting an individual; and (4) security awareness training. The personnel office is normally the first point of contact in helping managers determine if a personnel investigation is necessary for a particular position. See BPSSM Section 2.	Related CSRs: 1.10.5	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.5.6	An independent review or audit of the security controls of all Medicare systems and applications processing sensitive information is performed at least every three years.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying conduct of an independent review or audit at least every three years.	FISCAM IRS 1075
	Guidance: Periodic independent assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.	Related CSRs: 1.8.6	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.5.7	CMS Business Partner office facilities processing sensitive information are subjected to an annual self-assessment.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	CMS FISCAM IRS 1075
	Guidance: Annual self-assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.	Related CSRs: 2.12.1, 1.4.2, 1.8.6	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

2.5.8 Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

CMS
HIPAA
IRS 1075

Guidance: Inspection, self-assessment, and corrective action reports are an important means of identifying areas of noncompliance and remedial actions performed to correct noncompliance.

Related CSRs: 1.4.2

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

2.5.9 Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

CMS
IRS 1075

Guidance: The procedures are used to test the security system attributes.

Related CSRs: 1.4.2, 5.7.1

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

2.5.10 Sensitive information system development documentation is available, including security mechanisms and implementation.

Inspect system design and test documentation for an explanation of security mechanisms and how they are implemented.

FISCAM

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

Related CSRs: 6.3.7

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

2.5.11 Sensitive information system documentation contains the test policy, test plan, test procedures, and retest procedures, and it describes how and what mechanisms were tested, and the results.

Review the sensitive information system documentation for inclusion of required test documentation.

FISCAM

Guidance: A disciplined process for testing and approving new and modified systems prior to their implementation is essential to ensure systems operate as intended and that no unauthorized changes are implemented. Security is an integral part of the test.

Related CSRs: 6.3.1, 6.3.9

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

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

2.6.1 Security violations and activities, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.

1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM

Guidance: Audit functions should be activated to maintain critical audit trails and report unauthorized or unusual activity to the appropriate personnel.

Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 4.2.1, 4.2.4, 3.1.1, 10.2.3, 2.9.1

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

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

Guidance: Audit trails are a mechanism that help managers maintain individual accountability. By advising computer operators that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.

Related CSRs: 3.6.5, 5.2.6

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

	Control Technique	Protocol	Reference
2.6.3	Procedures instruct supervisors: (1) to monitor the activities of visitors to the work area (including CMS Business Partner employees from other work areas); and (2) to ensure that functions of the unit are performed only by employees assigned to the unit. Supervisors shall have procedures for handling questionable activities.	1. Confirm by inspection that the required procedures exist. 2. By inspection confirm that supervisors have specified procedures.	CMS

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

Related CSRs: 2.2.17

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

2.7 Owners of classified resources shall assign adequate classification to documentation and systems.

	Control Technique	Protocol	Reference
2.7.1	Resources are classified based on risk assessments. Classifications are documented and approved by an appropriate senior official, and are periodically reviewed.	1. Review resource classification documentation and compare to risk assessments. 2. Inspect audit data confirming that the required approval and review processes are consistently used.	FISCAM PDD 63

Guidance: Resource classification determinations flow directly from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing sensitive data or failing to protect the integrity of data supporting critical transactions or decisions.

Related CSRs: 1.7.1, 2.5.2, 1.8.3, 4.4.1

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

	Control Technique	Protocol	Reference
2.7.2	Access to sensitive information is on a strictly need-to-know basis. Contractors evaluate the need for the sensitive information before the data is requested or disseminated.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	CMS HIPAA IRS 1075

Guidance: The policies and procedures for limiting access ensure that properly authorized access is allowed based on an employee's need-to-know.

Related CSRs: 2.12.1, 2.5.3, 2.9.4

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

2.8 Resource owners shall identify authorized users and the level of authorization.

	Control Technique	Protocol	Reference
2.8.1	Security is notified immediately when system users are terminated or transferred.	1. Review relevant policies and procedures for inclusion and directed use of the required procedure. 2. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.	FISCAM

Guidance: Users who continue to have access to critical or sensitive resources pose a major threat, especially those who may have left under acrimonious circumstances.

Related CSRs: 1.10.4, 2.2.20, 2.9.9

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

	Control Technique	Protocol	Reference
2.8.2	All changes to security profiles by SSO or designated representative are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming routine identification and investigation of unusual activity. 3. Review a selection of recent profile changes and activity logs.	FISCAM

Guidance: Access controls should be documented, maintained on file, approved by senior managers, and periodically reviewed by resources owners to determine whether they remain appropriate.

Related CSRs: 9.3.4, 2.11.4, 3.1.1

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

	Control Technique	Protocol	Reference
2.8.3	SSOs or their designated representative review access authorizations and discuss any questionable authorizations with resource owners.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM PDD 63

Guidance: One method is for a listings of authorized users and their specific access needs should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security manager.

Related CSRs: 1.4.1, 2.2.15, 2.4.2, 3.3.3

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

	Control Technique	Protocol	Reference
2.8.4	The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a selection of users with dial-up access, review authorization and justification.	FISCAM

Guidance: Because dial-up access can significantly increase the risk of unauthorized access, it should be limited and the associated risks weighted against the benefits.

Related CSRs: 10.10.1

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

	Control Technique	Protocol	Reference
2.8.5	Owners periodically review access authorization listings and determine whether they remain appropriate.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM PDD 63

Guidance: The owner should identify the nature and extent of access to each resource that is available to each user. A good approach is to build an architecture matrix of personal and data access functions.

Related CSRs: 2.2.18, 1.4.1

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

	Control Technique	Protocol	Reference
2.8.6	Authorization lists and controls for restricted areas, such as the computer room, tape library, and workstation rooms, are maintained. Authorization lists show the following information: (1) who is authorized access to restricted areas; (2) who is authorized to operate the equipment; (3) which workstations are authorized to access the computer and computer records; and (4) who may maintain operating systems, utilities, and operational versions of application programs.	1. By inspection, confirm that authorization lists include the required information. 2. Inspect audit data confirming continuing maintenance of authorization lists and access controls for restricted areas.	CMS

Guidance: Authorization lists and controls for restricted areas should be part of doing business to restrict access to areas containing or processing sensitive information.

Related CSRs: 6.4.1, 2.2.2, 2.2.12, 2.2.23

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

2.8.7 Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. For a sample representing each type of computer operating system, and for standalone and each mode of network connection affecting banner display, observe that the warning banner on the sample computer is consistent with the documented procedure.

CMS
IRS 1075

Guidance: The log-on banner/screen warning banner warns the user that the system processes sensitive information and it is subject to monitoring each time they log-on.

Related CSRs: 10.8.3

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

2.8.8 Documented policies and procedures exist for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.

Review the appropriate documented policies and procedures for inclusion of the required rules.

HIPAA

Guidance: The policies and procedures used to grant different levels of access to sensitive information are based on an employee's need-to-know.

Related CSRs: 2.2.14

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

2.8.9 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to the SSO.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Policies and procedures should exist for authorizing access to information resources and for documenting such authorizations.

Related CSRs: 2.14.1, 2.2.15, 1.4.1, 2.4.2

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

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

2.9.1 Attempts to log on with invalid passwords are limited to 3 attempts.

1. Review security software password parameters.
2. Review pertinent policies and procedures.
3. Observe the system directed action in response to four invalid access attempts, confirming that the action is consistent with the documented policy.

FISCAM

Guidance: To prevent guessing of passwords, attempts to log on the system with invalid passwords should be limited.

Related CSRs: 2.6.1, 7.3.6

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

2.9.2 Use of names or words as passwords is prohibited.

Review relevant policies for inclusion and directed use of the required prohibition.

FISCAM

Guidance: The use of alphanumeric passwords reduces the risk that an unauthorized user could gain access to a system by using a computer to try dictionary words or names until the password is guessed.

Related CSRs: 1.1.1, 3.6.2

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.9.3	Users maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others, and report lost items immediately.	1. Interview a sample of users to confirm the required understanding and device possession. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM
	Guidance: Factors that affect the use of these devices include (1) the frequency that possession by authorized users is checked, and (2) users' understanding that they should not allow others to use their identification devices.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.9.4	The use of passwords and access control measures are in place to identify who accessed protected information and limit that access to persons with a need-to-know.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review Access Authorization Lists to confirm designation of all users allowed access to each separate security partition within the system (e.g. each platform root logon, each application relating to a unique separation of duties boundary, and each network device that supports direct logon). 3. Review documentation describing audit systems implemented to record all accesses to protected information. 4. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description. 5. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing. 6. Inspect a sample of access audit data supporting continuing use to the required process.	FISCAM HIPAA IRS 1075
	Guidance: Logical access controls should be designed to restrict legitimate users to the specific system(s), programs, and files they need and prevent others, such as hackers, from entering the system at all.	Related CSRs: 2.7.2, 2.2.16, 2.5.3, 2.11.4, 7.4.1, 7.4.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

	General Requirement Control Technique	Protocol	Reference
2.9.5	When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) Authentication is provided through ID and password encryption for use over public telephone lines; (2) Standard access is provided through a toll-free number and through local telephone numbers to local data facilities; and (3) Both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards should have both identification and authentication features and provides data encryption as well.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the specified controls for all dialup access to systems handling sensitive information. (Controls for packet switched network access are covered in other control techniques.) 3. Review audit data, including spot inspections, confirming that all the specified controls are applied to all dialup access. This includes review of all devices having potential access to sensitive information that are equipped with modems. 4. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.	FISCAM IRS 1075
	Guidance: The entity should have cost-effective physical and logical controls in place for protecting systems accessed remotely. The purpose of this CSR is to prevent unauthorized access or disclosure of PHI by implementing controls that reflect industry security standards. Without authentication, the system cannot verify the provider or supplier is who they claim to be. Without encryption, the system cannot protect the data while in transit. If the PHI is under the control of the business partner, it is expected they will provide reasonable protection. Where the business partner considers the cost is excessive, they should seek alternative controls that will be more cost effective. For example; if modems are already implemented without encryption, the business partner may propose software encryption as an alternate control. In the event the business partner is unable to find less expensive alternatives, they need to provide a cost to meet this CSR in a Safeguard. CMS will then consider the cost and associated risk in funding these solutions over time.	Related CSRs: 3.6.1, 3.6.3, 10.8.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.9.6	Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff after a predetermined amount of time (normally 15 minutes) and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), or (d) telephone callback procedure.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation supporting implementation of the required controls. 3. Review a sample of audit data confirming continuing use of the required controls.	HIPAA
	Guidance: Procedures should be in place to authenticate users before granting them access to the system or application.	Related CSRs: 7.3.5, 10.8.2, 10.10.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.9.7	Password files are encrypted.	1. View a sample dump of password files (e.g., hexadecimal printout). 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM
	Guidance: Encrypting the password file reduces the risk that it could be accessed and read by unauthorized individuals.	Related CSRs: 10.5.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

General Requirement
Control Technique | **Protocol** | **Reference**

2.9.8 Vendor-supplied passwords are replaced immediately.

1. For a sample of applications and network devices, attempt to log on using common vendor-supplied passwords. These default passwords are usually documented in the associated manuals.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM

Guidance: Vendor supplied passwords are known by every hacker and they are usually the first passwords tried by hackers.

Related CSRs: 3.6.2, 10.10.1

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

2.9.9 Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.

1. Review pertinent policies and procedures.
2. Review documentation of such comparisons.
3. Interview security managers.
4. Make comparison using audit software.

FISCAM

Guidance: Policies and procedures should exist for terminating system access for all users no longer requiring access. This does not have to be an automated process but any process that is automatically followed when a user is terminated or transferred.

Related CSRs: 1.10.4, 2.2.20, 2.8.1

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

2.9.10 Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed periodically--every 30 to 90 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least six alphanumeric characters in length and prohibited from reuse for at least 6 generations.

1. Interview users.
2. Review security software password parameters.
3. Observe users keying in passwords.
4. Attempt to log on without a valid password. Make repeated attempts to guess passwords.
5. Assess procedures for generating and communicating passwords to users.
6. Review pertinent policies and procedures.

CMS
FISCAM
HIPAA

Guidance: Policies and procedures should exist that implement these minimum password requirements.

Related CSRs: 7.3.2, 10.10.1

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

2.9.11 Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords are utilized where supported by existing operating systems.

1. Inspect a sample of workstations running each type of operating system in use to confirm that the required process is in use.
2. Review configuration documentation supported implementation of the required feature.

CMS
FISCAM
HIPAA

Guidance: Workstation time-outs and password protected screen savers are important access controls used to prevent unauthorized users from accessing the system using the logged-on users credentials.

Related CSRs: 7.3.5, 10.10.1

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

2.9.12 Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.

Review documentation establishing that authorization control exists, and includes the required feature.

HIPAA

Guidance: The mechanisms are used to authenticate users before granting them access permissions to the system or application.

Related CSRs: 2.4.1

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

2.9.13 If a CMS business partner is part of a larger organization, the business partner must implement policies and procedures that protect CMS sensitive information from unauthorized access by the larger organization.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Interview a sample of users to confirm the required understanding and access authorizations.

HIPAA

Guidance: Review security policies and procedures for business partner access.

Related CSRs:

☐ ***SS*** ☐ ***PartB*** ☐ ***PartA*** ☐ ***Dmerc*** ☐ ***DC*** ☐ ***CWF***

2.10 Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure.

2.10.1 Security software is used to restrict access. Access to security software is restricted to security administrators only.

1. Review documentation describing the security software in use for restriction of access to data files and software programs.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation of security software parameters that limit access to the security software to security administrators.

FISCAM

Guidance: The most commonly used means of restricting access to data files and software programs is through the use of access control software, also referred to as security software. Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted.

Related CSRs: 3.6.4, 3.6.5

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

2.10.2 Security administration personnel set parameters in security software to provide access as authorized and restrict assess that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files and operating system files. Standardized naming conventions are used for resources.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Perform penetration testing by attempting to access and browse computer resources.
3. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
4. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.
5. Review documentation describing the standardized naming conventions in use for resources.

FISCAM

Guidance: The most commonly used means of restricting access to data files and software programs is through the use of access control software. Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Generally, access control software provides many access control options that must be activated and tailored to the entity’s needs in order to be effective.

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

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

	General Requirement Control Technique	Protocol	Reference
2.10.3	Updating of data is restricted to authorized employees.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List(s) identifying employees who are authorized to update data. 3. Inspect a sample of audit data confirming that the required process is consistently used 4. Review documentation of the control used to restrict of data updating to authorized employees.	CMS
Guidance:	Logical access controls provide a technical means of controlling what information users can access (in accordance with relevant policy), the programs they can run, and the modifications they can make. Logical access controls may be implemented internally to the computer system being protected or may be implemented in external devices.	Related CSRs: 7.4.1, 7.4.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.10.4	Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, uncatalog, scratch, and rename a file.	1. Review documentation of the process used to provide the specified control over routines that modify the status of a file. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.	CMS
Guidance:	Utilities for file access and related processing need controls in place.	Related CSRs: 7.4.1, 7.4.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.10.5	Inactive users accounts are monitored and removed when not needed.	1. Review a sample of audit data confirming continued operation of the required control. 2. Review documentation describing how the required control is implemented.	FISCAM
Guidance:	Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Inactive accounts should be monitored and revoked when no longer required.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.11	Logical controls shall be implemented for databases and DBMS software.		
2.11.1	Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	1. Review security system parameters. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM
Guidance:	Access control settings should be implemented in accordance with the access authorizations established by the resource owners.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
2.11.2	Access and changes to DBMS software are controlled.	1. Review the controls protecting DBMS software. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM HIPAA
Guidance:	Access control settings should be implemented in accordance with the access authorizations established by the resource owners. In addition, DBMS software changes should be protected from unauthorized changes through the use of logical access controls.	Related CSRs: 6.5.2, 6.6.1, 3.4.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

2.11.3 Use of DBMS utilities is limited.

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

FISCAM

Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. In addition, use of DBMS utilities should be protected through the use of logical access controls and audit trails.

Related CSRs:

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

2.11.4 Database management systems (DBMS) and data dictionary controls have been implemented that: (1) restrict access to data files at the logical data view, field and field-value level; (2) control access to the data dictionary using security profiles and passwords; (3) maintain audit trails/logs that allow monitoring of changes to the data dictionary; and (4) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.

1. Interview database administrator.
2. Test controls by attempting access to restricted files.
3. Review pertinent policies and procedures.

FISCAM

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

Related CSRs: 6.3.5, 6.6.1, 2.8.2, 2.9.4

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

2.12 Sensitive material shall be protected.

2.12.1 Access to sensitive information is limited to those who are authorized by law or regulation. Physical and systemic barriers are reviewed/reported. Assessments are conducted of facility security features.

1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

IRS 1075
PDD 63

Guidance: Physical security controls augment technical means for controlling access to information and processing. It is important to review the effectiveness of physical access controls, both during normal business hours and at other times - particularly when an area may be unoccupied. Effectiveness depends on both the characteristics of the control devices used (e.g., keycard-controlled doors) and the implementation and operation.

Related CSRs: 1.4.2, 2.5.3, 2.5.7, 2.7.2

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

2.12.2 Medicare data is not released to outside personnel unless their identity is verified.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

CMS

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

Related CSRs: 1.3.2, 1.3.8

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

2.13 Suspicious access activity shall be investigated and appropriate action taken.

2.13.1 SSOs investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.

Protocol: Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.

Reference: FISCAM

Guidance: Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations should be investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur, repair any damage. The seriousness of the issue should determine what disciplinary actions might be taken. A good approach is to tie these violations/accidents into performance evaluations.

Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1

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

2.13.2 Violations are summarized and reported to senior management.

1. Interview senior management and personnel responsible for summarizing violations.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Inspect audit data confirming that the required process is consistently used.

Reference: FISCAM

Guidance: The frequency and magnitude of security violations and corrective actions taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the entity's operations, and any need for additional controls.

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

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

2.13.3 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

Reference: FISCAM

Guidance: Once it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur and repair any damage that has been done.

Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.2, 3.1.1, 3.4.1

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

2.13.4 Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

Reference: CMS
IRS 1075

Guidance: The process of inventorying and documenting missing tapes containing sensitive information should be integrated into the normal business processes of the organization.

Related CSRs:

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

2.14 Owners shall determine disposition and sharing of data.

2.14.1 Standard forms are used to document approval for archiving, deleting, and sharing data files.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect standard approval forms.

Reference: FISCAM

Guidance: A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard forms should be used and maintained on file to document the users' approvals.

Related CSRs: 1.3.8, 2.8.9

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

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

Examine documents authorizing file sharing and file sharing agreements.

FISCAM

Guidance: Resource owners should determine if, with whom, and by what means information resources can be shared. When files are shared with other entities, it is important that (1) data owners understand the related risks and approve such sharing, and (2) receiving entities understand the sensitivity of the data involved and safeguard the data accordingly. This should normally require a written agreement prior to the sharing of sensitive information.

Related CSRs:

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

3. *System Software*

3.1 Inappropriate or unusual activity shall be investigated and appropriate actions taken.

3.1.1 Policy defines investigation of inappropriate or unusual activity and guidelines for appropriate actions to be taken.

Review system operational policies and guidelines.

FISCAM

Guidance: The possibility of damage or alteration to the system software, application software, and related data files should be investigated and needed corrective actions taken. For example, policy guideline actions should include notifying the resource owner of the violation.

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

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

3.1.2 Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).

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

FISCAM

Guidance: A good approach is to include the evaluation of the software control techniques in the risk assessment with annual reviews. If there are any suspicious functions or processes occurring then the suspicious event should be investigated immediately.

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

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

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

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

FISCAM

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

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

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

	General Requirement **Control Technique**	**Protocol**	**Reference**
3.1.4	Systems programmers' activities are monitored and reviewed.	1. Determine that system programmer supervisors are supervising and monitoring their staff. 2. Review documentation supporting the supervising and monitoring of systems programmers' activities. 3. System Programmer and/or System Administrators need supervisor rights to make modifications. These personnel need additional controls in place to prevent misuse of these rights.	FISCAM
Guidance:	System programmers and/or system administrators need supervisor rights to make modifications. These personnel need additional controls in place to prevent misuse of these rights. All programmers need monitoring. The monitoring controls which are set globally for all programmers include: displaying sign-on information to the user which indicates the date and time of their last sign-on and any unauthorized sign-on attempts; monitoring the number of minutes of terminal inactivity before either canceling a job or disconnecting from a terminal; setting a limit to a user's ability to logon to multiple terminals with the same userid at the same time; the ability to distinguish between local and remote sign-on in order to prevent remote accesses completely or require normal logon security for remote access; and supervisors and managers review the activities process.	Related CSRs: 4.2.1, 4.2.4, 3.2.3, 4.4.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
3.1.5	Systems support alarm features to provide immediate notification of predefined events.	1. Review security plan to determine use of audit logs and alarms set points. 2. Review audit logs.	HIPAA
Guidance:	It is a good practice to have an automated audit system perform the immediate notification.	Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
3.2	Policies and techniques shall be implemented for using and monitoring system utilities.		
3.2.1	Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.	1. Verify that the appropriate responsibilities have been defined. 2. Interview systems programmers regarding their responsibilities.	FISCAM
Guidance:	Security training is adjusted to the level of the system programmer's responsibilities.	Related CSRs: 1.1.4	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
3.2.2	Responsibilities for monitoring use are defined and understood by technical management.	1. Verify that the appropriate responsibilities are defined. 2. Interview technical management regarding their responsibilities.	FISCAM
Guidance:	Security training is adjusted to the level of the technical management's responsibilities.	Related CSRs: 1.1.4	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
3.2.3	Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	1. Interview management and systems personnel. 2. Verify the existence and current version of the appropriate policies and procedures.	FISCAM
Guidance:	It is a good practice to identify access for various programs and utilities, monitoring, and written policies and procedures. As part of the System Security Plan, policies and procedures for using and monitoring the use of system software utilities should be defined and documented.	Related CSRs: 3.1.4, 4.4.2	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		

3.2.4 The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).

1. Determine whether logging occurs and what information is logged.
2. Review logs.
3. Using security software reports, determine who can access the logging files.

FISCAM

Guidance: The output report log is a good management tool to assist in tracking the usage of sensitive system utilities. The policy and procedures for the sensitive system utilities are normally depicted in the system security plan.

Related CSRs: 1.9.4, 9.6.5

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

3.3 Access authorizations shall be appropriately limited.

3.3.1 Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.

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

FISCAM

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

Related CSRs: 1.1.8

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

3.3.2 Policies and procedures for restricting access to systems software exist and are up-to-date.

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

FISCAM

Guidance: Access to system software is restricted to a few system programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly.

Related CSRs: 1.9.4

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

3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.

Determine the last time the access capabilities of system programmers were reviewed.

FISCAM

Guidance: Security skill needs are accurately identified and included in job descriptions. The duties from the job description should be compared to the SSO's security access list and the security audit logs. If these functions do not match then management should take corrective action(s). The review memo should be provided to the SSO for inclusion in the System Security Profile.

Related CSRs: 3.1.3, 1.1.2, 2.8.3

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

3.3.4 Justification and management approval for access to systems software is documented and retained.

1. Interview system manager and security administrator.
2. Review appropriate documentation, and verify that it is retained.

FISCAM

Guidance: The SSO normally maintains an approved Access Control Listing (ACL) for all systems that process or transmit sensitive data. The individual's supervisor provides justification and approval to the SSO. The ACL is part of the System Security Profile.

Related CSRs: 1.9.5

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

3.4 Installation of system software shall be documented and reviewed.

	Control Technique	Protocol	Reference
3.4.1	Installation of all system software is logged to establish an audit trail/log and is reviewed by data center management.	1. Interview data center management about their role in reviewing system software installations. 2. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.	FISCAM

Guidance: A good process for monitoring and documenting migration of system software is in the change management process for the organization.

Related CSRs: 9.7.1, 9.8.1, 9.8.2, 9.8.3, 6.5.2, 2.3.1, 2.11.2, 2.13.3, 4.7.6, 6.3.5, 6.3.6, 6.3.10, 6.6.1, 6.7.1, 6.8.1, 10.7.3, 10.10.1

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

	Control Technique	Protocol	Reference
3.4.2	Migration of tested and approved system software to production use is performed by an independent library control group.	Interview management, systems programmers, and library controls personnel, and determine who migrates approved system software to production libraries, and whether versions are removed from production libraries.	FISCAM

Guidance: A good process for monitoring and documenting the migration of system software is in the change management process for the organization.

Related CSRs: 6.8.2, 4.7.6

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

	Control Technique	Protocol	Reference
3.4.3	Vendor-supplied system software is supported by the vendor.	Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.	FISCAM

Guidance: A good approach is to include vendor maintenance with the purchase of the software.

Related CSRs:

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

	Control Technique	Protocol	Reference
3.4.4	Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	1. Interview management and systems programmers about scheduling and giving advance notices when system software is installed. 2. Review recent installations and determine whether scheduling and advance notification did occur. 3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.	FISCAM

Guidance: If possible, a good approach to scheduling major installations of system software is during off hours. This creates minimal impact on operations and provides time to back out the installation if errors occur. Notification can be provided several days in advance via email.

Related CSRs:

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

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

Guidance: Outdated versions are kept in a library other than the production library. In order to prevent redundant execution of older versions, they should be deleted from production and moved elsewhere. Storage for outdated versions may be part of the Contingency Plan reconstitution efforts.

Related CSRs:

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

3.4.6 All system software is current and has current and complete documentation.

1. Review documentation and test whether recent changes are incorporated.
2. Interview management and system programmers about the currency of system software, and the currency and completeness of software documentation.

FISCAM

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

Related CSRs: 1.9.4

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

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

3.5.1 New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation.

1. Determine the procedures used to test and approve system software prior to its implementation.
2. Select a few recent systems software changes and review audit data confirming that the specified process was followed.
3. Review procedures used to control and approve emergency changes.
4. Select some emergency changes to system software and test whether the indicated procedures were in fact used.

FISCAM

Guidance: This should be documented and provided in the Change Management process. Change management standards, proper controls, processes, and procedures will provide for appropriate testing prior to implementation.

Related CSRs:

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

3.5.2 Policies and procedures exist and are up-to-date for identifying, selecting, installing and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.

1. Interview management and systems personnel.
2. Verify that policies and procedures are current, and contain the required information.

FISCAM

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

Related CSRs: 1.9.4, 1.4.1, 1.8.4

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

3.5.3 Procedures exist for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.

1. Review procedures for identifying and documenting system software problems.
2. Interview management and systems programmers.
3. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.

FISCAM

Guidance: A good approach is to automate the software problem tracking processes. Monthly tracking reviews will assist in controlling any issues.

Related CSRs: 1.9.4

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

3.5.4 New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.

1. Determine what authorizations and documentation are required prior to initiating system software changes.
2. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.

FISCAM

Guidance: A preformatted change request process provides efficiency and assists in the accuracy of the change tracking processes.

Related CSRs: 6.6.1, 6.7.1, 4.7.6

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

3.5.5 Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.

Verify the existence of checkpoint and restart capabilities.

CMS

Guidance: Checkpoints and Restart capabilities on jobs will assist in meeting performance goals.

Related CSRs: 4.7.6

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

3.5.6 Procedures exist for controlling emergency changes. These procedures include: (1) authorizing and documenting emergency changes as they occur, (2) reporting the changes for management review, and (3) review of the changes by an independent IT supervisor.

1. Interview an independent IT supervisor who has previously reviewed changes.
2. Verify the existence of emergency change procedures.
3. Interview system managers.

FISCAM

Guidance: A good approach is to include emergency procedures in the change management process as well as appropriate procedures in the Contingency Plan

Related CSRs: 5.6.2, 5.7.2, 6.6.1, 1.9.4

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

3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.

3.6.1 All accesses to system software files are logged by automated logging facilities.

Review sample accesses to system software files to confirm automated logging facilities.

FISCAM

Guidance: This is part of the application and system access controls. Included could be an alerting process when an automated notification process can identify suspicious logging or file changes occur.

Related CSRs: 2.2.24, 2.9.5

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

3.6.2 Vendor-supplied default login IDs and passwords have been disabled.

1. Inquire whether disabling has occurred.
2. Test for default presence using vendor standard IDs and passwords.

FISCAM

Guidance: Disabling default passwords and removing the obsolete software should be part of enhancing security (hardening) process when new software or systems are installed.

Related CSRs: 2.9.8, 1.9.4, 10.10.1, 2.9.2

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

3.6.3 Remote access to the system master console is restricted. Physical and logical controls provide security over all workstations that are set up as master consoles.

1. Determine what terminals are set up as master consoles and what controls exist over them.
2. Test to determine if the master console can be accessed, or if other terminals can be used to mimic the master console and take control of the system.

FISCAM

Guidance: Only authorized personnel should have access to the master console(s). If all the procedures in access control are followed and proper physical control is provided then the master consoles should be secure.

Related CSRs: 1.9.4, 2.2.12, 2.9.5

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

3.6.4 Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access is generally limited to primary and backup systems programmers.

1. Obtain a list of all system software on test and production libraries used by the entity.
2. Verify that access control software restricts access to system software.
3. Using security software reports, determine who has access to system software files, security software, and logging files. Reports should be generated by the auditor, or at least in the presence of the auditor.
4. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.

FISCAM
HIPAA

Guidance: Security skill needs are accurately identified and included in job descriptions. After necessary personnel have been identified, then corresponding access control software must be matched and implemented.

Related CSRs: 2.10.1, 1.1.2

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

3.6.5 The operating system is configured to prevent circumvention of the security software and application controls.

1. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.
2. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.

FISCAM

Guidance: System hardening should be part of operating system installation. Once the system is hardened then the security should be baselined and periodically updated. Additionally, an Intrusion Detection System, when possible, should be implemented for real time monitoring. A Host Intrusion Detection System would assist in preventing circumvention of controls.

Related CSRs: 2.10.1, 2.10.2, 2.2.1, 2.6.2

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

3.6.6 The operating system's operational status and restart integrity is protected during and after shutdowns.

1. Interview the system manager.
2. Verify the protection of the operating system during and after shutdowns.

CMS

Guidance: A good practice is to have qualified personnel standing by when systems are taken offline and when shutdowns occur. The QA team could provide a standard list for restart.

Related CSRs: 5.2.9

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

4. *Segregation of Duties*

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

4.1.1 Application run manuals provide instruction on operating specific applications.

1. Inspect run manuals for inclusion of the required instructions.
2. Employees demonstrate that documentation is understood and adhered to.

FISCAM

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

Related CSRs: 4.1.3

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

	General Requirement Control Technique	Protocol	Reference
4.1.2	Operators are prevented from overriding file labels or equipment error messages.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing how controls meet the specified requirement. 3. Employees demonstrate that documentation is understood and adhered to.	FISCAM
Guidance:	A good approach is to provide periodic training in operating procedures, which should cover operator-prohibited activities.	Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5	
	☐ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
4.1.3	Detailed, written instructions exist to guide personnel in performing their duties. Computer operator manuals provide guidance on system startup and shut down procedures, emergency procedures, system and job status reporting, and operator prohibited activities. Application-specific manuals provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.	1. Determine that the required operator and security manuals exist, and that they provide the required documentation. 2. Determine that documents are understood and adhered to by staff.	FISCAM
Guidance:	Manuals should contain instructions on all procedures which the employee is expected to perform on a regular basis and in an emergency situation.	Related CSRs: 5.6.2, 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 4.1.1, 3.1.3, 3.1.5	
	☐ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
4.1.4	The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing use of the specified approval process.	CMS
Guidance:	The approval process should be documented and reviewed periodically.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
4.1.5	Duties in critical control and financial functions are split. (e.g., establish special controls involving more than one person over blank and voided checks.)	1. Interview supervisors in the critical control and financial areas. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS
Guidance:	Duties should be documented in job descriptions. Appropriate separation of data will assist in preventing fraud. See BPSSM information on fraud protective measures.	Related CSRs:	
	☐ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
4.2	Active supervision and review shall be provided for all personnel.		
4.2.1	All operator activities on the computer system are recorded on an automated history log.	1. Determine by review that an automated history log exists on each computer system, and that they record all operator activities. 2. Interview supervisors to confirm that supervisors routinely review history log.	FISCAM
Guidance:	The history log serves as an audit trail and should be reviewed routinely by supervisors.	Related CSRs: 2.1.1, 2.6.1, 3.1.4	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		

Category: ***Segregation of Duties***

General Requirement

Control Technique | **Protocol** | **Reference**

4.2.2 Personnel are provided adequate supervision and review, including each shift of computer operations.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming continuing supervision and review in accordance with the documented process.

FISCAM

Guidance: Supervision and review of personnel activities assure that these activities are performed in accordance with prescribed procedures, mistakes are corrected, and computers are used for authorized purposes.

Related CSRs: 1.4.1

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

4.2.3 System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.

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

FISCAM

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

Related CSRs:

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

4.2.4 Supervisors routinely review the history log and investigate any abnormalities.

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

FISCAM

Guidance: The history log serves as an audit trail.

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

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

4.3 Job descriptions shall be documented.

4.3.1 Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.

1. Review documentation establishing that existing documented job descriptions meet segregation of duty principles.
2. Inspect the effective dates of position descriptions to confirm that they are current.
3. Confirm by interview of the incumbents that documented job descriptions match actual current responsibilities and duties.

FISCAM

Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.

Related CSRs: 3.1.3

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

	Control Technique	Protocol	Reference
4.3.2	Documented job descriptions include definitions of the technical knowledge, skills and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	1. Confirm by review that job descriptions are documented, and that they meet the specified criteria. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM

Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department. Related CSRs: 5.1.2

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

4.4 Management shall review effectiveness of control techniques.

	Control Technique	Protocol	Reference
4.4.1	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM

Guidance: A good approach is a documented management review on an annual basis. Related CSRs: 3.1.2, 2.7.1

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

	Control Technique	Protocol	Reference
4.4.2	Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM

Guidance: A periodic employee performance review could be used to demonstrate compliance. Related CSRs: 3.1.4, 3.2.3

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

4.5 Physical and logical access controls shall be established.

	Control Technique	Protocol	Reference
4.5.1	Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	Review documentation establishing now physical and logical access controls accomplish the specified restriction.	CMS FISCAM

Guidance: This can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities. Related CSRs: 2.3.1

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

4.6 Employees shall understand their security duties and responsibilities.

	Control Technique	Protocol	Reference
4.6.1	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview employees to confirm that their job descriptions match their understanding of their duties and responsibilities, and that they carry out those responsibilities in accordance with their job descriptions.	FISCAM

Guidance: Employees should have access to their job descriptions and discuss during their performance evaluations. Related CSRs: 3.1.3

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

	Control Technique	Protocol	Reference
4.6.2	Local policy assigns senior management responsibility for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced and institutionalized within the organization.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM

Guidance: Senior management is responsible for assuring that employees understand their responsibilities. Related CSRs:

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

Category: ***Segregation of Duties***

General Requirement

Control Technique — **Protocol** — **Reference**

4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.

1. Review documented procedures identifying responsibilities for restricting access by job position in key operating and programming activities to confirm that these responsibilities are clearly defined.
2. Interview a sample of personnel identified as having the specified responsibilities to confirm that the responsibilities assigned are clearly understood and followed.
3. Employees demonstrate that documentation is understood and adhered to.

FISCAM

Guidance: A good approach is to develop a matrix identifying resources in relation to organizational access and job title.

Related CSRs:

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

4.7 Incompatible duties shall be identified and policies implemented to segregate these duties.

4.7.1 Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

Review approval controls.

FISCAM

Guidance: Compensating controls should be documented.

Related CSRs:

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

4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. No individual has complete control over incompatible transaction processing functions.

1. Review the required analyses for inclusion of the specified elements.
2. Confirm by review that the required analyses reflect current operations.

FISCAM

Guidance: Establish independent organizational groups with defined functions. Functions and related tasks performed by each unit should be documented.

Related CSRs:

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

4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.

1. Review documentation of process design establishing the specified separation of duties.
2. Confirm through interview, observation, and review of job descriptions for a sample of personnel, that these separation of duties requirements are met.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM

Guidance: Policy procedures and access approvals need to account for correct users of information systems. The initiating approval form can identify job descriptions that are involved for system and application access.

Related CSRs:

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

4.7.4 Policies and procedures for segregating duties exist and are up-to-date.

Confirm through inspection that the required policies and procedures exist and are consistent with current operations.

FISCAM

Guidance: Policies are documented, communicated, and enforced.

Related CSRs:

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

4.7.5 Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.

Confirm by review that documented operating procedures meet the required criteria.

FISCAM

Guidance: Documentation should be reviewed periodically and updated as needed.

Related CSRs:

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

4.7.6 Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) quality assurance/testing; (6) library management/change management; (7) computer operations; (8) production control and scheduling; (9) data control; (10) data security; (11) data administration; and (12) network administration.

1. Review the agency organization chart showing IS functions and assigned personnel.
2. Interview selected personnel and determine whether functions are appropriately segregated.
3. Review relevant alternative or backup assignments and determine whether the proper segregation of duties is maintained.
4. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.

FISCAM

Guidance: Manuals and job descriptions include support functions of each individual.

Related CSRs: 3.4.1, 3.4.2, 3.5.4, 3.5.5

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

5. *Service Continuity*

5.1 Adequate environmental controls shall be implemented.

5.1.1 Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known.

1. Examine facility maintenance records for history of water damage.
2. Interview site managers for knowledge of potential pumping related hazards and familiarity with mitigation procedures.
3. Interview a sample of operations staff to confirm familiarity with mitigation procedures for potential plumbing related problems.
4. Observe the operation, location, maintenance, and access to the air cooling systems condensate drains.
5. Observe whether water can enter through the computer room ceiling or pipes are running through the facility, and that there are water detectors on the floor.
6. Review relevant procedures for inclusion mitigation measures for any potential plumbing related problems.
7. Review the current risk assessment to confirm investigation of the potential for plumbing related problems, and review risk mitigation plans for any such risks identified.

FISCAM

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

Related CSRs:

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

5.1.2 Any behavior that may damage computer equipment is prohibited.

1. Review the risk assessment for identification of potentially hazardous employee activities.
2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment.
3. Review job descriptions to ensure there is guidance contained relative to destructive behavior.

FISCAM

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

Related CSRs: 4.3.2

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

Category: ***Service Continuity***

	General Requirement Control Technique	Protocol	Reference
5.1.3	Controls have been implemented to mitigate other disasters, such as floods, earthquakes and fire.	1. Review the risk assessment plan for consideration of the specified potential risks. 2. Review documentation of efforts to identify additional risks specific to the region, area, or facility. 3. Review documentation of risk mitigation planning covering all identified risks. 4. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.	FISCAM
	Guidance: The SSO should work in conjunction with the building engineer/maintenance. High risk items should be identified e.g., location of the flood plain.	Related CSRs: 1.8.4, 2.2.14, 5.6.3	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.1.4	Environmental controls are periodically tested.	1. Review the test plans for future tests. 2. Review test policies. 3. Review documentation supporting recent tests of environmental controls.	FISCAM
	Guidance: There should be a test plan for the testing of the environmental controls, e.g., humidistat.	Related CSRs: 5.7.1	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.1.5	Redundancy exists in the air cooling system.	1. Review facility design documentation confirming air cooling system redundancy. 2. Review maintenance records confirming primary and redundancy systems are operational. 3. Observe demonstrations of operation of primary and redundant cooling systems. 4. Review policy and procedures relevant to operation and maintenance of primary and redundancy air cooling systems	FISCAM
	Guidance: Only the critical components or subsystems of the entire air cooling system need to be redundant.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.1.6	Fire suppression and prevention devices have been installed and are working (e.g., smoke detectors, fire extinguishers and sprinkler systems).	1. Review facility drawings and other documentation documenting types and locations of the specified devices. 2. Review documentation of periodic inspections and maintenance of the specified devices and related systems to assure they are fully operational. 3. Review documentation supporting the qualifications of personnel inspecting and maintaining the specified devices and systems. 4. Observe that fire extinguishers, smoke detectors and sprinkler systems are in place and appear to be in working order.	FISCAM
	Guidance: A good approach is to have the fire department review the systems.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

5.1.7 An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down.

1. Review facility documentation confirming installation of an uninterruptible power system (UPS).
2. Review design and test data supporting the capacity of the system to support the facility technical load long enough to allow shut down with lose of no more that transactions in progress at the time primary power is lost.
3. Review documentation supporting existence of periodic test, and preventive maintenance consistent with system specifications.
4. Review policies and procedures for orderly shut down of the system within the time allowed by the available UPS capacity.
5. Interview a sample of operations personnel for familiarity with the orderly shut down process and applicable documented procedures.
6. Review documentation supporting periodic test of the orderly shut down process.
7. Observe that secondary power supplies exists.

FISCAM

Guidance: The facility managers should periodically verify the current computing power load and auxiliary requirements for change.

Related CSRs: 5.9.8, 5.10.1

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

5.2 A Contingency Plan shall be documented in accordance with CMS Contingency Plan Methodology.

5.2.1 The Contingency Plan provides for backup personnel so that it can be implemented independent of specific individuals.

1. Review the contingency plan to confirm inclusion of the specified provision.
2. Review documentation supporting timely availability of the backup personnel required by the contingency plan.
3. Talk with a random small sample of the designated backup persons to ensure that they understand their role in a contingency.

FISCAM

Guidance: Refer to Appendix B of the BPSSM.

Related CSRs: 5.8.1, 5.10.3

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

	General Requirement Control Technique	Protocol	Reference
5.2.2	User departments have developed adequate manual processing procedures for use until automated operations are restored.	1. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation. 2. Review the contingency plan for identification of the specified manual procedures. 3. Inspect the required manual procedures for consistency with the contingency plan. 4. Interview the relevant process managers to confirm familiarity with the required procedures. 5. Review test reports to determine that manual procedures have been tested, at least on a sample basis.	FISCAM
	Guidance: Determine that the manual procedures have been tested. Refer to Appendix B of the BPSSM.	Related CSRs: 1.8.4	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.2.3	The Contingency Plan clearly assigns responsibilities for recovery.	Review the Contingency Plan to confirm clear identification of specific responsibilities for all elements of recovery.	FISCAM
	Guidance: Ensure that individuals have been assigned to all the responsibilities that need to be executed during a contingency. Refer to Appendix B of the BPSSM.	Related CSRs: 3.6.4, 4.3.1, 4.6.1, 5.6.1	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.2.4	Contingency Plan consists of all components listed in the CMS Business Partner's Systems Security Manual.	1. Review Appendix C of the Business Partners Systems Security Manual. 2. Verify through inspection that the Contingency Plan includes the specified elements.	CMS FISCAM HIPAA
	Guidance: A business partner contingency plan contains the topics described in Appendix B of the Business Partners Systems Security Manual.	Related CSRs: 5.3.1, 5.4.1, 5.4.2, 5.5.1, 5.6.1, 5.8.1	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.2.5	Management and the SSO approve Contingency Plans.	1. Verify through inspection that all Contingency Plans have been approved by management and the SSO. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS FISCAM
	Guidance: It is important that the contingency plan be reviewed and approved by persons that are knowledgeable about the systems and environment so that nothing is missed in the plan.	Related CSRs: 5.7.2	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***
5.2.6	Management and the SSO are able to show how the organization responds to specific disasters/disruptions to: (1) protect lives, (2) limit damage, (3) protect sensitive data, (4) circumvent safeguards according to established bypass procedures, and (5) minimize the impact on Medicare operations.	1. Review documentation, CCTV tapes or other recordings. 2. Determine through interview that system manager(s) and the SSO can explain how the organization covers each of the specified requirements through its response to specific disasters/disruptions.	CMS FISCAM
	Guidance: A good approach might be to review documentation in the security profile to determine if the organization has responded properly to emergency situations (such as incidents) in the past.	Related CSRs: 5.5.1, 5.6.1, 5.6.2, 5.6.3, 5.6.4, 5.10.1, 2.6.2	
	☑ ***SS*** ☑ ***PartB***	☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF***

5.2.7 The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.

Review the Contingency Plan emergency response procedures for inclusion of the required provision.

CMS
HIPAA

Guidance: Ensure that this immediate entry action has been practiced during exercises and training.

Related CSRs: 1.1.7, 2.4.1, 2.4.2, 5.6.1, 5.6.4, 2.2.2

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

5.2.8 Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency plans are re-evaluated before proposed changes are approved.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming that contingency plans have been reevaluated before any proposed major modifications were approved.

CMS

Guidance: Change control management should provide for updates to the Contingency Plan.

Related CSRs:

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

5.2.9 Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.

1. Review documentation supporting the contention that existing contingency plans protect storage media from improper modification in the event of system failure.
2. Review documentation describing use of installed security and backup capabilities to reduce the potential for data loss and/or modification during a system failure.
3. Review documentation describing use of software procedures to reduce the potential for data loss and/or modification during a system failure.

CMS

Guidance: Throughout documentation review and testing, ensure that the safeguards protect data from modification if the system fails.

Related CSRs: 2.5.1, 2.14.2, 3.6.6, 6.4.1, 7.2.2, 9.3.3, 9.8.1, 5.11.2

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

5.2.10 The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.

1. Review test reports.
2. Verify through inspection that the contingency plan identifies the specified interfaces.

CMS

Guidance: Critical interfaces should be tested when the contingency plan is exercised.

Related CSRs:

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

5.3 Critical data and operations shall be identified and prioritized.

5.3.1 A list of critical applications, operations and data has been documented that: (1) prioritizes data and operations; (2) is approved by senior program managers; and (3) reflects current conditions.

1. Verify by inspection that the required, prioritized list has been prepared.
2. Verify by inspection that the list is approved by senior management.
3. Review documentation supporting the contention that the list reflects current conditions.
4. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM
HIPAA

Guidance: It is important to know what critical data and operations are needed to continue critical functions in an emergency.

Related CSRs: 1.9.7, 2.1.3, 5.4.4, 5.8.1

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

5.4 Data and program backup procedures shall be implemented.

5.4.1 System and application documentation are maintained at the off-site storage location.

1. Interview persons at the primary site who are responsible for storing documents off-site.
2. Review documentation supporting maintenance of the required off-site storage.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM

Guidance: Current systems and applications documentation should be available off-site in case the primary processing site is disabled.

Related CSRs: 5.7.3

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

5.4.2 Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data supporting consistent operation of the required rotation.
3. Verify by inspection the location of specific backup files.
4. Review documentation confirming successful periodic test of the ability to recover using backup files.

FISCAM
HIPAA

Guidance: Offsite backup files should be current to the point that operations would not be delayed or disrupted if the data or software were suddenly put into operation.

Related CSRs: 5.11.1, 5.9.8

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

5.4.3 The backup storage site is geographically removed from the primary site(s) and protected by environmental controls and physical access controls.

1. By inspection, verify that the backup storage facility is consistent with available documentation.
2. Review contingency plan test reports or exercise lessons learned reports to determine if the backup site functioned as planned.
3. Review documentation confirming that the backup storage site meets the stated requirements.

FISCAM

Guidance: It should be verified that the backup site can operate to process critical data and accomplish critical functions to allow business to progress during an emergency.

Related CSRs: 5.11.2

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

5.4.4 The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.

1. Observe the initiation of delivery of critical data from the primary site to the off-site facility.
2. Review the Contingency Plan to verify that it contains the specified elements.
3. Review records of data backups.

CMS
HIPAA

Guidance: Refer to Appendix B of the BPSSM.

Related CSRs:

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

5.4.5 A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.

An inventory of all equipment and software should be maintained, including the location and person responsible.

HIPAA

Guidance: A record should be use to track the movement all resources.

Related CSRs:

□ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

5.5 Emergency processing priorities shall be established.

Control Technique	Protocol	Reference
5.5.1 Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.	FISCAM HIPAA

Guidance: Processing priorities should exist for all critical functions and processes to be accomplished during an emergency. These should be periodically reviewed for accuracy.

Related CSRs: 5.3.1, 5.6.4

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

5.6 Management and staff shall be trained to respond to emergencies.

Control Technique	Protocol	Reference
5.6.1 Data center staff have received training and understand their emergency roles and responsibilities.	1. Interview a sample of data center staff to confirm their understanding of their roles in emergency response procedures. 2. Review training records to confirm required training has been conducted, and is consistent with the current procedures. 3. Review training plans for future training in emergency actions.	FISCAM

Guidance: There should be evidence that the data center staff has periodically received training relative to what to do in an emergency.

Related CSRs: 1.1.7

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

Control Technique	Protocol	Reference
5.6.2 Emergency procedures are documented.	By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan.	FISCAM HIPAA

Guidance: Procedures for use in an emergency should exist for automated and manual processes. They should be readily available. Refer to Appendix B of the BPSSM.

Related CSRs: 1.1.7, 2.2.14, 2.4.1, 3.5.6, 4.1.3, 5.2.7, 6.1.2

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

Control Technique	Protocol	Reference
5.6.3 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.	1. Review training records to confirm that the required training has been delivered periodically. 2. Review training plans for future training in emergency actions.	FISCAM

Guidance: These are procedures primarily for staff and management working in a data processing center environment.

Related CSRs: 1.1.7

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

Control Technique	Protocol	Reference
5.6.4 Emergency procedures are periodically tested.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming completion of the required testing. 3. Review future test plans to ensure that the emergency procedures are scheduled to be properly tested. 4. Interview data center staff.	FISCAM HIPAA

Guidance: Procedures for use during an emergency situation should be tested annually, or whenever major changes are made to the system environment. Refer to Appendix B of the BPSSM.

Related CSRs: 5.2.7, 5.5.1, 5.7.1

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

5.7 The contingency plan shall be annually reviewed and tested.

5.7.1 The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.

1. Review documentation of annual conduct of the required test.
2. Review documentation describing how the testing conditions simulate an emergency or disaster.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Review test plans for upcoming contingency plan testing, including lessons learned from the previous testing.

CMS
FISCAM
HIPAA

Guidance: It is advisable to conduct "live tests" of critical system processes to ensure they will function in an emergency.

Related CSRs: 5.6.4, 2.5.9

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

5.7.2 Contingency Plans are reviewed whenever new operations are planned or new safeguards contemplated.

1. Review the current contingency plan.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

CMS
FISCAM

Guidance: Contingency plans should be reviewed before system or process changes are made to determine the possible changes necessary to the contingency plan. Change Control Management should alert the contingency plan team to all changes.

Related CSRs: 1.9.5, 1.12.2, 3.5.6, 6.3.10

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

5.7.3 Several copies of the current Contingency Plan are securely stored off-site at different locations, including homes of key staff members. It is reviewed once a year, reassessed and, if appropriate, revised to reflect changes in hardware, software and personnel.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data supporting consistent annual review, reassessment, and appropriate revision of the contingency plan as specified.
3. Review documentation confirming the required off-site distribution and storage.

CMS
FISCAM

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

Related CSRs: 5.4.1, 5.9.3

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

5.7.4 Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review distribution records or interview senior management to ensure that they received the latest contingency plan test results and lessons learned information.

FISCAM

Guidance: Senior management should be informed in a timely manner of contingency plan test results and lessons learned so that they can direct appropriate actions to modify the plan or change test plans and procedures.

Related CSRs:

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

5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documents establishing that the contingency plan and related agreements are adjusted as specified.

FISCAM
HIPAA

Guidance: Following contingency plan testing it is advisable to review the test results and make modifications to the plan and related agreements with inside and outside organizations as quickly as possible.

Related CSRs:

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

5.8 Resources supporting critical operations shall be identified.

5.8.1 Resources supporting critical operations are identified and documented. Types of resources identified include: (1) computer hardware; (2) computer software; (3) computer supplies; (4) system documentation; (5) telecommunications; (6) office facilities and supplies; and (7) human resources.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect documents identifying resources supporting critical operations for inclusion of the specified resource types.

FISCAM

Guidance: It is important that resources needed to support critical operations during an emergency and recovery time periods be documented for availability to all concerned persons, and that they be reviewed for currency whenever the contingency plan is to be tested.

Related CSRs: 5.3.1, 2.1.3, 5.4.4, 5.9.8

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

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.1 Senior management periodically: (1) reviews and compares the service performance achieved with the goals; and (2) surveys user departments to see if their needs are being met.

1. Interview users.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review the performance records to ensure the goals are clearly stated in writing.

FISCAM

Guidance: To avoid a break in continuity of service, hardware performance should be evaluated frequently and users polled relative to level of service provided.

Related CSRs:

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

5.9.2 Problems and delays encountered, including the reason and elapsed time for resolution of hardware problems, are recorded and analyzed to identify recurring patterns or trends.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review samples of the required logs.
3. Review documentation supporting conduct of the required analyses.

FISCAM

Guidance: Hardware problems should be carefully analyzed in order to determine the maintenance needs and to prevent major failures.

Related CSRs:

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

5.9.3 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.

FISCAM

Guidance: Any changes to hardware equipment or software should be carefully reviewed, tested, and a schedule created for implementation of the changes. Peak workload periods should be avoided for implementation. Vendor supplied specifications normally prescribe the frequency and type of preventative maintenance to be performed.

Related CSRs: 1.9.1, 5.7.3, 6.3.4, 10.7.3, 6.6.1

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

5.9.4 Goals are established by senior management for the availability of data processing and on-line services.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming establishment of the required goals.

FISCAM

Guidance: Reasonable data processing goals should be set by management to guide the maintenance and problem analysis relative to hardware performance and availability.

Related CSRs:

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

5.9.5 Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.

1. Review records of past advanced notifications.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.

FISCAM

Guidance: Notice of at least 2 days should be given to users relative to hardware changes.

Related CSRs: 5.7.3, 10.7.3

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

5.9.6 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.

FISCAM

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

Related CSRs: 2.2.24

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

5.9.7 Records are maintained on the actual hardware performance in meeting service schedules.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect the required records.

FISCAM

Guidance: Records should be kept for all critical hardware components in the system, such as mainframe, server, disc unit, tape unit, controllers, front end processors, and operations consoles and workstations.

Related CSRs:

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

5.9.8 Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.

1. Review documentation confirming availability of spare or backup hardware for support of applications designated as critical or sensitive.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review operations and maintenance documentation to confirm that levels of available backup or spare hardware have been sufficient to support system availability objectives.

FISCAM

Guidance: In an emergency, or for unscheduled maintenance, spare and backup hardware units, and the appropriate switchover software, should be available to prevent interruption of critical processes.

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

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

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

Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.

Related CSRs: 1.9.1, 1.4.1, 1.8.4

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

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

Guidance: Maintenance records are kept and reviewed for trends and lessons learned. They can be organized by type unit or subsystem. Review meetings should be held with major vendors reviewing the statistics.

Related CSRs: 1.8.4, 1.9.5

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

	Control Technique	Protocol	Reference
5.9.11	Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	1. Inspect hardware maintenance schedules 2. Review documentation supporting the contention that the hardware maintenance schedule complies with vendor specifications. 3. Review maintenance records to confirm completion of hardware maintenance in accordance with the schedule. 4. Review documentation supporting the contention that the manner of performing maintenance minimizes the impact of maintenance on operations.	FISCAM

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

Related CSRs:

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

5.10 Arrangements shall be made for alternate data processing and telecommunications facilities.

	Control Technique	Protocol	Reference
5.10.1	Arrangements and agreements have been established for a backup data center and other needed facilities that: (1) are in a state of readiness commensurate with the risks of interrupted operations; (2) have sufficient processing capacity and; (3) are available for use.	1. Review documentation supporting the contention that alternate facilities have sufficient processing capacity. 2. Inspect agreements established to confirm coverage of all identified alternate facilities. 3. Review documentation identifying facilities required for alternate data processing and telecommunications. 4. Review documentation supporting the contention that alternate facilities are in the required state of readiness. 5. Review documentation supporting the contention that alternate facilities are available for use.	CMS FISCAM

Guidance: Agreements should be such that the services to be provided in an emergency are clearly defined and understood by all parties concerned. Security and protection of information should be addressed in these agreements.

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

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

	Control Technique	Protocol	Reference
5.10.2	Alternate telecommunication services have been arranged.	Review documentation confirming the arrangement of alternate telecommunication services.	FISCAM

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

Related CSRs: 5.7.5, 5.8.1

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

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

Guidance: Arrangements should address persons that may need to come from distant locations and those that are local but may need to stay at or near the data processing site.

Related CSRs:

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

5.11 A contingency plan shall exist for any standalone computer workstations that specifies where backup data, software, and current operating procedures are stored.

	Control Technique	Protocol	Reference
5.11.1	A Contingency Plan is available for each standalone computer workstation that specifies where backup data and software are stored. A single plan can cover more than one workstation.	1. Review the required contingency plan(s) to confirm inclusion of the specification of storage location(s) for backup data and software. 2. Review documentation confirming that the specified plan is available for each standalone workstation.	CMS

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

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

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

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

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

Related CSRs: 5.2.9, 5.4.3, 5.4.2, 5.9.8

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

5.12 Detection of malicious software shall be performed.

	Control Technique	Protocol	Reference
5.12.1	The CMS Business Partner shall use special software to accomplish malicious software identification, detection, protection, and elimination.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the required software is installed and operational in accordance with documented policy.	FISCAM HIPAA

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

Related CSRs: 1.1.1, 1.9.1, 2.2.24, 10.2.2

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

6. *Application Software Development and Change Control*

6.1 Emergency changes to application software shall be promptly tested and approved.

6.1.1 Emergency changes are documented and approved by appropriate operations management, formally reported to appropriate computer operations management for follow-up, and approved after the fact by appropriate programming and user management.

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

FISCAM

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

Related CSRs: 6.3.2, 6.6.1

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

6.1.2 Emergency change procedures are documented.

Review the documentation of emergency change procedures.

FISCAM

Guidance: Ensure that the procedures for making emergency software changes are current.

Related CSRs: 1.1.7, 2.4.1, 2.4.2, 3.5.6, 5.6.2, 1.9.3, 10.7.3

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

6.2 Use of public domain and personal software shall be restricted.

6.2.1 Clear policies restricting the use of personal and public domain software have been developed and are enforced.

1. Review the required policies, and verify that they are enforced.
2. Interview the security administrator..
3. Interview users.

FISCAM

Guidance: It may be necessary to periodically randomly inspect disk drives and servers to ensure that only approved personal or public domain software is resident.

Related CSRs:

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

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.1 Test plans are documented and approved that define responsibilities for each party involved.

1. Interview test manager, and others as deemed necessary.
2. Interview the system manager.
3. Verify that test plans are documented and approved, and define the required responsibilities.

FISCAM

Guidance: Persons involved in testing may include system analysts, programmers, quality assurance analysts, data base managers, security analyst, network analyst, software library control staff, users, system administrators, and test planners.

Related CSRs: 2.5.11

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

6.3.2 Unit, integration and system testing are performed and approved in accordance with the test plan. A sufficient range of valid and invalid conditions are applied.

1. For the software change request selected: (1) Compare test documentation with related test plans; (2) Analyze test failures to determine if they indicate ineffective software testing.
2. Review test plan to ensure that it addresses test levels and conditions.

FISCAM

Guidance: The test plan should be carefully reviewed to ensure that all necessary levels of testing are described and that test conditions are clearly defined. Test standards should be available.

Related CSRs: 2.5.10, 2.5.11, 3.5.1

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

6.3.3 A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live test data are not to be used in testing.

1. Confirm the restrictions in the use of live data.
2. Interview test programmers.
3. Interview the system manager.
4. Verify that test data will meet all processing criteria.

FISCAM

Guidance: Tests should be conducted in an environment that simulates the conditions that are likely to be encountered when the changed software is implemented. A set of test transactions and data should be developed that contains examples of the various types of situations and information that the changed program will have to handle, including invalid transactions or conditions to make certain the software recognizes these transactions and reacts appropriately. In addition, the system's ability to process the anticipated volume of transactions within expected time frames should be tested.

Related CSRs: 1.9.1, 2.5.10, 2.5.11, 3.5.1, 4.7.6, 5.9.3, 6.4.4, 9.8.1

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

6.3.4 Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.

1. Review documentation of all required departments for prompt and accurate updating.
2. Interview the system manager.
3. Interview the document control person (librarian).

FISCAM

Guidance: Documentation used by hardware, software, operations, and systems persons should reflect the latest system and software environment.

Related CSRs: 1.9.1, 1.9.7, 2.5.1, 2.5.10, 3.4.6, 5.4.1, 5.8.1, 6.5.1, 5.9.3, 1.9.3, 10.7.3

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

6.3.5 Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.

1. Interview the software programming supervisor.
2. Review documented software changes to verify the tracing process.

FISCAM

Guidance: There should be documentation that provides a logical trace from initial requirements and specifications through to finished tested code, with no gaps in the trace path.

Related CSRs: 2.11.2, 2.11.4, 3.5.6, 6.1.1, 6.6.1, 10.7.3, 6.7.2, 3.4.1

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

6.3.6 Program changes are moved into production only upon documented approval from users and system development management.

1. Interview user management.
2. Verify the documented approval of program changes before production implementation.
3. Interview system development management.

FISCAM

Guidance: Persons that understand the changes made to software and the test results of those changes should approve moving the software from development into production.

Related CSRs: 3.4.5, 3.4.1

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

6.3.7 Test results are reviewed and documented.

1. Verify that test results are reviewed and documented.
2. Interview the system manager.

FISCAM

Guidance: All test data, transactions, and results should be saved and documented. This will facilitate future testing of other modifications and allow a reconstruction if future events necessitate a revisit of the actual tests and results.

Related CSRs: 2.5.10

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

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

	General Requirement Control Technique	Protocol	Reference
6.3.8	Changes to detailed system specifications are prepared by the programmer and reviewed by the appropriate supervisor or manager.	1. Interview the programming supervisor. 2. Review documented changes to system specifications.	FISCAM
	Guidance: Specification changes are very important and can have far reaching effects. The requests for these should be carefully reviewed and approved by knowledgeable persons.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
6.3.9	Test plan standards have been developed and are followed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).	1. Ensure through observation or interviews that during testing persons/groups fulfilled their responsibilities. 2. Review test plan standards, and confirm that they follow all levels of testing and responsibilities. 3. Interview department supervisors to verify their compliance with test plan standards.	FISCAM
	Guidance: A good practice is to have independent tests performed.	Related CSRs: 1.4.4, 2.5.11	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
6.3.10	Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	1. Interview the system programmers and/or system administrator. 2. Determine when the last production program change was reviewed, and how often. 3. Interview data center management and/or the security administrator.	FISCAM
	Guidance: Access controls and change controls should be periodically reviewed and/or tested to ensure their proper function.	Related CSRs: 3.1.2, 3.1.3, 3.3.3, 3.4.1, 4.4.1, 7.3.6	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
6.3.11	A system development life cycle (SDLC) methodology has been developed that: (1) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (2) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; and (3) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements.	1. Interview the system manager. 2. Confirm that the SDLC includes the three required elements.	FISCAM
	Guidance: Ensure that a current SDLC methodology exists, addresses security has been reviewed, and is being followed.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
6.3.12	Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	1. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current. 2. Examine training plans and records. 3. Interview the programming staff and the software staff.	FISCAM
	Guidance: Training plans and materials should exist for training in SDLC methodology.	Related CSRs:	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		

6.3.13 Security policy assigns responsibility to Application System Managers for ensuring that appropriate administrative, physical and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.

1. Interview system programmers and administrators.
2. Interview the application system managers.
3. Review the documented policy to ensure that the required responsibilities are assigned.

CMS
HIPAA

Guidance: Tests should be performed and test reports should be reviewed to ensure that safeguards that protect software from unauthorized modification have been tested.`

Related CSRs: 1.5.2, 1.5.6, 1.9.5, 5.7.2

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

6.4 Access to program libraries shall be restricted.

6.4.1 Access to all programs, including production code, source code, and extra program copies, 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. Determine if the access controls are implemented and working.

FISCAM
HIPAA

Guidance: Separate software libraries should be established and only the library control group should be allowed move programs between libraries. Programmers should only have access to the programs they are assigned.

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

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

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

Select a few program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tape.

FISCAM

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

Related CSRs: 1.3.12, 2.2.8, 2.2.23, 2.8.6

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

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

1. Monitor libraries in use.
2. Verify that source code exists for a selection of production load modules by: (1) comparing compile dates; (2) recompiling the source modules; and (3) comparing the resulting module size to production load module size.

FISCAM

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

Related CSRs: 2.10.2

☑ ***SS*** □ ***PartB*** ☑ ***PartA*** □ ***Dmerc*** ☑ ***DC*** □ ***CWF***

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

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

FISCAM

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

Related CSRs: 2.10.2, 3.4.5, 6.8.2

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

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

6.5.1 Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.

1. Examine procedures for distributing new software.
2. Check implementation orders for a sample of changes.

FISCAM

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

Related CSRs: 1.9.5, 3.5.1, 6.3.4

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

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

Examine procedures for distributing new software.

FISCAM

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

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

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

6.6 Programs shall be automatically labeled and inventoried.

6.6.1 Library management software is used to produce audit trails/logs of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.

1. Interview personnel responsible for library control.
2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures.
3. Review software change control policies and procedures.

FISCAM

Guidance: Software controls should be easily monitored and audited. Library management of software helps ensure that differing versions are not accidentally misidentified.

Related CSRs: 6.3.5, 2.11.2, 2.11.4, 3.5.4, 3.5.6, 5.9.3, 6.1.1, 6.3.5, 10.7.3, 10.10.1, 6.8.2, 3.4.1

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

6.7 Authorizations for software modifications shall be documented and maintained.

6.7.1 Change requests are approved by both system users and data processing staff.

1. Determine if the change requests for past changes have been approved.
2. Interview software development staff.
3. Identify recent software modifications and determine whether change request forms were used.

FISCAM

Guidance: A good practice is to convene the change-control board to assure all appropriate personnel provide input and approval for software modifications and document the approval of the proposed changes.

Related CSRs: 3.5.4, 3.4.1

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

6.7.2 Software change request forms are used to document requests and related approvals.

Examine a selection of software change request forms for approvals.

FISCAM

Guidance: The forms should be designed such that they help ensure that change requests are clearly communicated . The authorization form may be maintained as a paper or softcopy item.

Related CSRs: 3.3.4, 6.3.5

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

6.8 Movement of programs and data among libraries shall be controlled.

6.8.1 Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.

1. Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared.
2. Examine some of the images of stored code that has been changed.

FISCAM

Guidance: An independent library control group should make the image comparisons.

Related CSRs: 3.4.1

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

6.8.2 A group independent of the user and programmers controls movement of programs and data among libraries.

Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.

FISCAM

Guidance: Prior to moving software from a test to production environment, an independent review of the changes developed and tested should be made.

Related CSRs: 2.10.2, 3.4.2, 6.3.9, 6.4.2, 6.4.4, 6.6.1

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

7. *Application System Authorization Controls*

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

7.1.1 For batch application systems, a batch control sheet is prepared for a group of source documents and includes; date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

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

FISCAM

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

Related CSRs:

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

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

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

FISCAM

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

Related CSRs: 1.1.8

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** □ ***DC*** □ ***CWF***

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

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

FISCAM

Guidance: It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents. Pre-numbered documents help/prevents missing or lost documents.

Related CSRs: 2.6.1, 2.13.1

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

7.2 Master files shall be used to identify unauthorized transactions.

7.2.1 Before transactions are processed, they are verified using master files of approved vendors, employees, etc., as appropriate for the application.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: It is a good practice to verify the transaction is applicable before any transactions are processed. For example, a procurement system requires approved vendors prior to processing of transactions.

Related CSRs:

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

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

	General Requirement Control Technique	Protocol	Reference
7.2.2	Master files and program code that does the verification are protected from unauthorized modification.	1. Identify and observe the procedures employed that protect master files and program code. 2. Review the documented procedure covering the protection of master files and program code. 3. Inspect audit data confirming that the required process is consistently used. 4. Review documentation of software controls used in providing the required protection.	FISCAM
	Guidance: The organization should maintain an application protection policy regarding the protection and modification of application master files and program code. A recommendation could be to include the policy in the application change management process or part of the organization's security profile.	Related CSRs: 5.2.9, 2.6.1, 2.13.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
7.3	Data entry workstations shall be secured and restricted to authorized users.		
7.3.1	All transactions are logged as entered, along with the User ID of the person entering the data.	1. Observe the processing of sample transactions, to ascertain that they are being logged correctly. 2. Review the documented procedure prescribing transaction logging.	FISCAM
	Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the data entry process is correct.	Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
7.3.2	Each operator is required to use a unique password and identification code before being granted access to the system.	1. Interview a sample of management and data entry personnel to confirm consistent use of the documented procedure. Confirm that there is no sharing of passwords or identification codes. 2. Review documented login procedure. 3. Observe a sample of data entry login.	FISCAM
	Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses, including the use of password and identification control.	Related CSRs: 2.9.10	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
7.3.3	When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Observe physical area during non-business hours.	FISCAM
	Guidance: Review the workstation policy/guidelines.	Related CSRs: 1.13.1, 2.2.12	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		
7.3.4	Data entry workstations are connected to the system only during specific periods of the day, which corresponds with the business hours of the data entry personnel.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation use. 3. Observe workstation use.	FISCAM
	Guidance: Review the workstation policy/guidelines.	Related CSRs: 1.13.1	
	☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***		

7.3.5 Each workstation automatically disconnects from the system when not used after a specific period of time.

1. Inspect audit data confirming that the required process is consistently used.
2. Review documented procedure for workstation configuration and use.
3. For a sample of workstation types, observe operation of the automatic disconnect process.

CMS
FISCAM

Guidance: Review the workstation policy/guidelines. Additionally, it is a good practice to review the audit logs to validate the workstation disconnect functionality.

Related CSRs: 1.13.1, 2.6.1, 2.13.1, 2.9.11, 2.9.6

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

7.3.6 Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the online access process is correct.

Related CSRs: 6.3.10, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1, 2.9.1

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

7.3.7 Data entry workstations are located in physically secure environments.

1. Review System Security Plan.
2. Observe location of workstations.

FISCAM

Guidance: Workstations processing or connected to systems processing sensitive data are located in physically secure areas.

Related CSRs: 2.2.12

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** □ ***DC*** □ ***CWF***

7.4 Users shall be limited to a set of authorized transactions.

7.4.1 Authorization profiles for users limit what transaction data entry personnel can enter.

1. Review audit controls used to assure continued application of the required procedure.
2. Review documented procedure for data entry to confirm enforcement of the required limitation.

FISCAM

Guidance: Review the application processing policy/guidelines.

Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4

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

7.4.2 Authorization profiles for users or workstations limit what transactions can be entered.

1. For a sample of each type of restricted workstation, observe attempted entry of a prohibited transaction by a logged on user who has the user permissions required to enter the transaction.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation of configuration management assuring continued operation of the required controls.
4. Review documents designating transactions authorized from each workstation.

FISCAM

Guidance: The supervisors should address limitations in access for inclusion in the ACL.

Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4

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

7.5 Exceptions shall be reported to management for review and approval.

7.5.1 Exceptions, based on parameters established by management, are reported for their review and approval.

1. Inspect audit data confirming that the required process is consistently used.
2. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.

FISCAM

Guidance: An exception report lists items requiring review and approval. These items may be valid, but exceed parameters established by management. For, example, in a disbursement system, all disbursements exceeding $20,000 could be reported to management for their review and approval before the disbursements are released.

Related CSRs: 1.13.1

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

7.6 Independent reviews of data shall occur before entering the application system.

7.6.1 Procedures are in place for a multilevel review of CMS sensitive input data before it is released for processing.

1. Review documented procedure for pre-processing of data.
2. Interview a sample of supervisors and control unit personnel to confirm use of the process.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: It is a good practice to validate the authorization list and to have a preformatted review list in place for processing CMS sensitive data.

Related CSRs:

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

7.6.2 Data control unit personnel monitor data entry and processing of source documents.

1. Interview management and data control unit personnel to confirm use of the process.
2. Review documented data entry and processing procedures.
3. Observe data entry and processing procedures.

FISCAM

Guidance: The data control unit is the quality assurance personnel group that validates the data on the source documents before the data is entered. Additionally, this group can monitor the data entry process for accuracy.

Related CSRs: 8.4.5, 8.5.1, 8.5.2

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

7.6.3 Data control unit personnel verify that source documents are properly prepared and authorized.

1. Inspect audit data confirming that the required process is consistently used.
2. Interview management and data control unit personnel to confirm use of the process.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Observe data control unit personnel performing the verification process.

FISCAM

Guidance: The data control unit is the quality assurance personnel group that validates the data on the source documents before the data is entered. Additionally, this group can monitor the data entry process for accuracy.

Related CSRs: 8.4.5, 8.5.1, 8.5.2

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

8. *Application System Completeness Controls*

8.1 Computer sequence-checking shall be implemented.

8.1.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review reports of missing or duplicate transactions.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: An alteration to the data files should be investigated and needed corrective actions taken. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation so that timely action(s) can be taken.

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

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

8.1.2 Sequence checking is used to identify missing or duplicate transactions.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: The possibility of alterations, missing transactions or duplicate transactions can occur if sequence numbers are not properly processed. If a sequence number is missing it may have been deleted or misplaced. The missing or duplicate data files should be investigated and corrective actions taken. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation.

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

☑ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

8.1.3 Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.

1. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers.
2. Review the documented procedure that prescribes the assigning of unique sequence numbers.
3. Inspect audit data confirming that the required process is consistently used.
4. Verify, though documentation review, that the application contains automatic routines for checking sequence numbers and appropriate reports/alerts are generated when serial numbers are not processed in sequence or duplicated.
5. Interview the system owner and determine what policies and corrective action are in place when a sequence number error occurs.

FISCAM

Guidance: This is a function of the processing application. The application developer or vendor should verify the existence of transaction serial numbers being assigned, and sequence number checking routines or modules included in the application.

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

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

8.1.4 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Serial numbers for source documents assist in the tracking of source documents. Additionally, the sequence of the serial numbers processed shows that a source document has not been inadvertently missed or an unauthorized transaction has been inserted into the process.

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

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

8.2 Computer matching of transaction data shall be implemented.

8.2.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.

1. Verify the application has an assigned system owner.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Inspect audit data confirming that the required process is consistently used.
4. Verify the application has the ability to insert the preassigned source document numbers matched with the associated data.

FISCAM

Guidance: The possibility of an alteration to the data files should be investigated and needed corrective actions taken. For example, within the policy guidelines, actions should include notifying the resource owner of the violation.

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

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

8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.

1. Verify that a system owner has been designated and when errors occur, that person is notified.
2. Review the program specifications that describe the computer matching process.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: The purpose of this CSR is to ensure that data input was completed thoroughly and nothing was duplicated or left out. The possibility of an alteration to the data files should be investigated and needed corrective actions taken. For example, within the policy guidelines, actions should include notifying the resource owner of the violation.

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

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

8.2.3 For high-value, low-volume items, individual transactions or source documents are compared with a detailed listing of items processed by the computer.

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

FISCAM

Guidance: This process is application dependent, but should be automated as much as possible. If an automated function is not available for the software, then consideration for developing such a process would improve the security of the application. High value items need special attention.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

8.3 Reconciliations shall show the completeness of the data processed for the total cycle.

8.3.1 Reconciliations are performed to determine the completeness of transactions processed, master files updated and outputs generated.

1. Inspect audit data confirming that the required process is consistently used.
2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.
3. Review the documented procedure describing the reconciliation process.

FISCAM

Guidance: This process is application dependent, but should be automated as much as possible.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

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

8.4 Reconciliations shall show the completeness of data processed at points in the processing cycle.

8.4.1 Record counts and control totals are established over time and entered with transaction data, and subsequently reconciled to determine the completeness of data entry.

1. Review the documented procedures for the data entry process.
2. Review a sample of data control reports for completeness of data entry.
3. This process is application dependent, but should be automated as much as possible. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.

FISCAM

Guidance: The application should be tracking each transaction and reconciling any differences with the data being entered. (commonly called "run-to-run control totals")

Related CSRs: 2.1.3, 2.1.5, 2.1.6

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

8.4.2 Trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed.

1. Verify that the application contains routines for process checking. The checking process should be included in applicable trailer labels.
2. Interview the supervisory application programmer to determine that system controls are in place as prescribed by the application programs.
3. Inspect audit data confirming that the required process is consistently used.
4. Review the program specifications describing the reconciliation process for accurate data entry.

FISCAM

Guidance: Trailer labels may include any number of tracking or checking techniques. The Trailer labels verify the accuracy of the process, but not the data entry accuracy. If the data is entered correctly and the data is processed completely, then there should not be errors in the output.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

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

8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.

1. Review the documented procedures describing the reconciliation process for data entry.
2. Interview the supervisory application programmer to determine implementation of automatic reconciliation in completion of computer job runs.
3. Inspect audit data confirming that the required process is consistently used.
4. Verify bends and processing errors are reconciled between the completion of one job and before the start of the next job. The reconciliation process should not stop all batch processing.

FISCAM

Guidance: This process is largely application dependent, but should be automated as much as possible. If an automated function is not available for the software, then consideration for developing such a process would improve the security of the application.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

☑ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

8.4.4 System interfaces require that the sending system's output control counts equal the receiving system's input counts.

1. Review the documented procedure describing the reconciliation process between systems.
2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: As systems have become more integrated over the years, a file produced by one application may be used in another application. It is important to reconcile control information between the sending and receiving applications.

Related CSRs: 2.1.3, 2.1.5, 2.1.6

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

8.4.5 A data processing control group receives and reviews control total reports and determines the completeness of processing.

1. Review the documented procedure describing the data control group's function.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Performing the comparison of control numbers is commonly referred to as balancing, and should be done automatically by the computer, although some older systems may rely on manual balancing procedures. The control numbers for the balancing at key points should be documented, such as being printed on a control totals report, and should be reviewed by the data processing control group that monitors the completeness and accuracy of processing.

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

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

8.5 Record counts and control totals shall be implemented on an IT System.

8.5.1 For on-line or real time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness of data entry and processing.

1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented procedures for the data control and data entry process for inclusion of the required process.

FISCAM

Guidance: This is part of the quality assurance process. Since the processing is on-line or real-time, the system can not be taken down for validation of processing. The only way to validate the processing accuracy is to take a snap shot or monitor the processing for accuracy by taking a sampling over a period of time.

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

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

8.5.2 User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.

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

FISCAM

Guidance: In general, user-prepared totals established over source documents and data to be entered can be carried into and through processing. The computer can generate similar totals and track the data from one processing stage to the next and verify that the data was entered and processed as it should have been.

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

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

9. *Application System Accuracy Controls*

9.1 Erroneous data shall be reported back to the user departments for investigation and correction.

9.1.1 Errors are corrected by the user originating the transaction.

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

FISCAM

Guidance: Some systems may use error reports to communicate to the user department the rejected transactions in need of correction. More modern systems will provide user departments access to a file containing erroneous transactions. Using a computer terminal or workstation, users can initiate corrective actions. The user responsible for originating the transaction should be responsible for correcting the error.

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

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

9.1.2 Error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.

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

FISCAM

Guidance: A good approach to tracking errors and developing procedures to minimize errors would be a detailed error list for managers and supervisors to track and expand corrective actions. Error messages should clearly indicate what the error is and what corrective action is necessary.

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

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

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

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

FISCAM

Guidance: As part of the formal security program, policies should be in a procedures document with system security features for error-correction procedures included. All corrections should be reviewed and approved by supervisors before being reentered into the system, or released for processing if corrected from a computer terminal or workstation.

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

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

9.2 Automated entry devices shall be used to increase data accuracy.

9.2.1 Effective use is made of automated entry devices to reduce the potential for data entry errors.

Review the documentation explaining how the specified objective is met.

FISCAM

Guidance: The use of automated entry devices (e.g., optical or magnetic ink character readers) can reduce data error rates, as well as speed the entry process. IRS' use of preprinted labels, showing the taxpayer's name, address, and social security number is such an example. This information can be entered without keying the data, which ensures a more accurate and faster process. A good approach validating compliance would be to document the security features of the system that spells out the characteristics of the automated data entry devices so that an audit of the procedures and devices can easily be evaluated.

Related CSRs: 2.2.16

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

9.3 Rejected transactions shall be controlled with an automated error suspense file.

9.3.1 Rejected data are automatically written on an automated suspense file and held until corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error; (2) date and time the transaction was processed and the error identified; and (3) the identity of the user who originated the transaction.

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

FISCAM

Guidance: As part of the formal security program, policies should be delineated in a procedures document with system security features for error-correction procedures included. A security audit review process should be documented and implemented.

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

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

9.3.2 A control group is responsible for controlling and monitoring rejected transactions.

1. Review the documented procedure describing the control group's responsibilities and duties.
2. Interview a sample of the control group to confirm operational responsibilities match those documented.

FISCAM

Guidance: A good approach would be to document the security features of the system that spells out system monitoring characteristics and the reasons for transaction rejections. Corrective action procedures should be documented and evaluated as well.

Related CSRs:

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

9.3.3 General controls effectively protect the suspense file from unauthorized access and modification.

Review the documentation describing how general controls provide the required protection of the suspense file.

FISCAM

Guidance: General controls should protect the suspense file from unauthorized access and modification, in order for the auditor to be able to rely on this control technique to reduce audit risk. A good approach would be to document the security features of the system, spelling out system monitoring characteristics and the action taken when policies are not followed.

Related CSRs: 5.2.9, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

9.3.4 The suspense file is purged of transactions as they are corrected.

1. Review the documented procedure for the error correction process to confirm inclusion of the specified process.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: The suspense file should be purged of the related erroneous transaction as the correction is made. Record counts and control totals for the suspense file should be adjusted accordingly. Suspense files are normally created as the result of data needing to be input into the system or a correction to data errors.

Related CSRs: 2.8.2

☑ ***SS*** □ ***PartB*** □ ***PartA*** □ ***Dmerc*** □ ***DC*** □ ***CWF***

9.3.5 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.

1. Review the documented procedure for suspense file processing and transaction reconciliation.
2. Observe the suspense file process to confirm that the documented procedure is followed.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Record counts and control totals should be developed automatically during processing of erroneous transactions to the suspense file and used in reconciling the transactions successfully processed. A control group should be responsible for controlling and monitoring the rejected transactions. The records count is a good management tool that assists in the administration of vital resources used to reconcile security transaction processing.

Related CSRs: 8.2.2

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** □ ***DC*** ☑ ***CWF***

9.3.6 The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected errors.

1. Review the documented suspense file procedure for inclusion of the specified processes.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Periodically, the suspense file should be analyzed to determine the extent and type of transaction errors being made, and the age of uncorrected transactions. This analysis may indicate a need for a system change or some specific training to reduce future data errors. The suspense file is a good management tool that assists in the administration of vital resources used to reconcile transaction processing.

Related CSRs: 9.1.2, 9.3.1, 8.2.2, 9.5.1, 9.6.7, 9.6.8, 3.1.5

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** □ ***DC*** □ ***CWF***

9.4 Source documents shall be designed to minimize errors.

9.4.1 The source document is well-designed to aid the preparer and facilitate data entry. Transaction type and date field codes are preprinted on the source document.

1. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry".
2. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.

FISCAM

Guidance: A good approach is to have needed data entry information succinctly formatted to facilitate ease of data entry.

Related CSRs: 1.9.4

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

9.5 Overriding or bypassing data validation and editing shall be restricted.

9.5.1 Overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

1. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: As part of the formal security program, policies should be delineated in a procedures document with system security features for error-correction procedures included. A security audit review process should be documented and implemented.

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

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

9.6 Output production and distribution shall be controlled.

9.6.1 Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design.

1. Review the documented procedure assigning responsibility for output production and distribution.
2. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.

FISCAM

Guidance: Security policies are distributed to all affected personnel to include system and application rules, rules to clearly delineate responsibility, and rules to describe expected behavior of all with access to the system.

Related CSRs: 1.4.4

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

9.6.2 The computer system automatically checks the output message before displaying, writing, and printing to make sure the output has not reached the wrong workstation device. A connection must be established to a specific device (workstation, printer, etc.) and verified by the system before transmitting data.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming use of the required process.
3. Review documentation describing how the required control is implemented.

FISCAM

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.

Related CSRs: 9.8.1, 9.8.2

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

9.6.3 The data processing control group, or some alternative, has a schedule by application that shows: (1) when outputs are completed; (2) when they need to be distributed; (3) who the recipients are; and (4) the copies needed. The group then reviews output products for general acceptability and reconciles control information to determine completeness of processing.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect the required schedule to confirm inclusion of the required elements.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted. The data control group becomes the baseline for that standard by which the output quality is measured.

Related CSRs: 1.5.2, 1.5.5

□ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***

9.6.4 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review sample printed reports to verify that it contains the elements required in the Control Technique.

FISCAM

Guidance: The printed report name, time, and date are good management tools to assist in the tracking of completed tasks.

Related CSRs:

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

9.6.5 Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review logs and check sample output, to verify that the required information is recorded.

FISCAM

Guidance: The output report log is a good management tool to assist in the tracking of completed tasks.

Related CSRs: 1.5.2, 3.2.4

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

9.6.6 Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.

1. Inspect audit data confirming that the required process is consistently used.
2. Review the documented procedure describing the output process and supervisory review.

FISCAM

Guidance: The printed reports are good management tools to assist in the tracking of completed tasks. Related CSRs: 1.5.2

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

9.6.7 A control log of output product errors is maintained, including the corrective actions taken.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review the control log and confirm that it contains the required information.

FISCAM

Guidance: The control log, with the suspense file, provides statistics on corrective action required and actions taken. This assists management in the status and use of its personnel and equipment resource tracking. Additionally, product errors may effect the implementation of a change request with appropriate security issues that can be addressed. Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

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

9.6.8 Output from reruns is subjected to the same quality review as the original output.

1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted. Related CSRs: 2.1.2, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1

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

9.7 Reports showing the results of processing shall be reviewed by users.

9.7.1 Users review output reports for data accuracy, validity, and completeness. The reports include error reports, transaction reports, master record change reports, exception reports and control totals balance reports.

1. Review the documented procedure describing the review process and detailed report constituency.
2. Inspect audit data confirming that the required process is consistently used.
3. Review sample reports to confirm that they include the required elements specified in the Control Technique.

FISCAM

Guidance: The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness. Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.4.1, 3.1.5

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

9.8 Programmed validation and edit checks shall identify erroneous data.

9.8.1 The following are protected from unauthorized modifications: (1) Program code for data validation and editing and associated tables or files; (2) Program code and criteria for test of critical calculations; and (3) Exception criteria and the related program code. Programs perform limit and reasonableness checks on critical calculations.

1. Review the documented procedure describing the protection provided program code, files, or tables.
2. Observe the actions or procedures in place that protect program code, files, or tables.

FISCAM

Guidance: Before an auditor can rely on the entity's data validation and editing checks that are meant to reduce the audit risk, the auditor must determine the adequacy of the general controls over those checks. To be effective, the general controls should protect the program code and any related tables associated with the validation and edit routines from unauthorized changes. Related CSRs: 5.2.9, 9.6.2, 3.4.1

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

9.8.2 Programmed validation and edits include checks for: (1) reasonableness; (2) dependency; (3) existence; (4) mathematical accuracy; (5) range; (6) check digit; (7) document reconciliation; and (8) relationship or prior data matching.

1. Review the documented procedure describing programmed validation and edits for inclusion of the specifically required checks.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM

Guidance: Programmed validation and edit checks are, for the most part, the most critical and comprehensive set of controls in assuring that the initial recording of data into the system is accurate. For example, programmed validation and edit checks can effectively start as the data are being keyed in at a computer workstation using preformatted computer screens.

Related CSRs: 9.6.2, 3.4.1

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

9.8.3 Validation and editing are performed at the computer workstation during data entry or are performed as early as possible in the data flow and before updating the master files. All data fields are checked for errors before rejecting a transaction.

1. Review the documented procedure describing the specified validation and editing process.
2. Inspect audit data confirming that the required process is consistently used.
3. Observe the validation and edit process.

FISCAM

Guidance: Validation of the accuracy of data assists in the integrity of the data being processed.

Related CSRs: 3.4.1

☑ ***SS*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***Dmerc*** ☑ ***DC*** □ ***CWF***

9.9 When appropriate, preformatted computer workstation screens shall be used for data entry.

9.9.1 Preformatted computer workstations screens are utilized and allow prompting for data to be entered and editing of data as it is entered.

1. Review documented procedure specifying preformatted workstation screens, and describing screen prompts.
2. Observe a sample of workstation screens as personnel are processing data.
3. Interview the system administrator to confirm that the required feature is universally available..

FISCAM

Guidance: A good approach is to have needed data entry information and workstation screens succinctly formatted to facilitate ease of data entry. Standards do promote efficiency and accuracy.

Related CSRs:

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

10. *Network*

10.1 LAN/Computer Room Access Controls shall be in place.

10.1.1 An access list of personnel authorized to access a data center to process sensitive data is controlled.

1. By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center.
2. Review audit data confirming control of access lists in accordance with documented procedures.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

CMS

Guidance: Ensure that only personnel with a need-to-know have access to the list.

Related CSRs: 2.2.23

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

10.1.2 Physical access to enclosures housing network equipment is restricted.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Select a sample of network equipment locations representative of the range of types of physical locations within each facility. For these sample equipment, confirm that access to them is restricted in accordance with the documented procedure.

CMS

Guidance: Ensure that access to the area where the network equipment is located is controlled.

Related CSRs:

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

10.2 Network system security shall be monitored for deficiencies.

10.2.1 Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation identifying devices selected to provide the specified logging function.
3. By inspection of a sample of the logs, confirm that they include network and system activity.

CMS

Guidance: Ensure that logs are kept of network activity.

Related CSRs:

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

10.2.2 Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network.

1. Confirm by inspection that virus-scanning software is installed.
2. Confirm by inspection that virus-scanning software is installed.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Review documentation identifying designated critical network entry points.

CMS

Guidance: A formal virus protection program should be established at the Network level.

Related CSRs: 5.12.1

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

10.2.3 Intrusion detection software is implemented providing real-time identification of unauthorized use, misuse, and abuse of computer assets by internal network users and external hackers.

1. Review alarm and alert functions of any firewalls and other network perimeter access control systems to insure they are properly enabled.
2. Review operating system, user accounting, and application software audit logging processes on all host and server systems to insure they are properly enabled.
3. Review relevant policies and procedures for inclusion of the required process.
4. Review sample of intrusion detection audit logs for servers and hosts on the internal, protected, network.

CMS

Guidance: Intrusion-detection mechanisms should be monitoring the system constantly. Failsafes and processes to minimize the failure of the primary security measures should be in place at all times.

Related CSRs: 2.6.1

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

10.3 Facsimile and E-mail shall be controlled.

	Control Technique	Protocol	Reference
10.3.1	Telephone numbers of the facsimile machines receiving sensitive information are verified before transmitting data.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect logs confirming conduct of the required verification.	CMS IRS 1075

Guidance: A good approach might be a policy that requires verification of the receiving facsimile machine's telephone number.

Related CSRs:

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

	Control Technique	Protocol	Reference
10.3.2	When sending or receiving sensitive fax information, have a trusted staff member at both sending and receiving fax machines, or have a locked room for the fax machine with custodial coverage over outgoing and incoming transmissions.	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS IRS 1075

Guidance: a good approach might be a policy that states "If a locked room with custodial coverage is unavailable, trusted staff members are required to be at both the transmitting and receiving machines prior to transmittal."

Related CSRs:

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

	Control Technique	Protocol	Reference
10.3.3	Policy exists identifying appropriate use of the E-mail system by employees, and procedures exist to enforce E-mail security, privacy, and message integrity	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.

Related CSRs:

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

	Control Technique	Protocol	Reference
10.3.4	Security policy exists and audit reviews include checks, to assure that system administrators and others with special system level access privileges are prohibited from reading the E-mail messages of others unless authorized on a case by case basis by appropriate management officials.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the audit process for operation in accordance with the documented process.	CMS

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Ensure that policy exists and it contains the necessary checks with regards to audit reviews.

Related CSRs:

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

	Control Technique	Protocol	Reference
10.3.5	Fax procedures for sensitive information require a cover sheet that explicitly provides guidance to the recipient, which includes: (1) Notification of sensitive data and need for protection, and (2) Notice to unintended recipients to telephone the sender, collect if necessary, to report the disclosure and confirm destruction of the information.	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS IRS 1075

Guidance: Establish a formal procedure generating and attaching the required fax cover sheet.

Related CSRs:

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

10.4 Cryptographic tools shall be controlled.

	Control Technique	Protocol	Reference
10.4.1	Sensitive information being electronically transmitted must be protected. Two acceptable methods for transmitting sensitive information over telecommunications devices: (1) encryption and (2) guided media.	1. Confirm by inspection that documented controls are in place and operational. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of controls used to assure protection of electronically transmitted sensitive information. 4. Review documentation establishing approval of the protection methods utilized.	FISCAM HIPAA IRS 1075

Guidance: Ensure that a means of protecting sensitive information during transmittal has been implemented. Guided media is generally acceptable for internal transmissions within protected facilities. Encryption is typically required for transmission outside of protected facilities or through uncontrolled or public facilities or systems.

Related CSRs:

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

	Control Technique	Protocol	Reference
10.4.2	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs when no other means of protection exists.	1. Review documentation establishing that the required protection has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM HIPAA

Guidance: In some cases—especially those involving telecommunications—it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs, both while these data and programs are “in” the computer system and while they are being transmitted to another computer system or stored on removable media, such as floppy disks, which may be held in a remote location.

Related CSRs:

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

10.5 Adequate Network password policies shall be implemented.

	Control Technique	Protocol	Reference
10.5.1	Passwords are transmitted and stored using secure protocols and algorithms.	1. Review documentation of controls used to assure that all systems remain configured to use the specified feature. 2. Review documentation explaining how this feature is implemented on each network and local computing environment. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM

Guidance: Ensure that passwords are not transmitted as plain-text.

Related CSRs: 2.9.7, 10.10.1

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

10.6 Internet Security Policies shall be made available.

Control Technique	Protocol	Reference
10.6.1 CMS Business Partner's Internet connections must be in accordance with the CMS Internet Security Policy. When a determination for Internet use has been made, it shall include at a minimum of Triple 56-bit DES (defined as 112-bit equivalent) for symmetric encryption, 1024-bit algorithms for asymmetric systems, and 160-bit for the emerging Elliptical Curve systems (CMS Internet Security Policy, dated November 24, 1998).	1. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement. 2. Review documentation describing protections to assure that the only interconnections allowed between the Internet and networks carrying sensitive information are the specified virtual private network connections. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review documentation describing the approved authentication process used to allow establishment of the virtual private network connection to a local network or other system carrying sensitive information.	CMS

Guidance: At present, the internet may not be used for CMS sensitive data. Related CSRs:

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

10.7 Configuration Control Policy shall be documented and available.

Control Technique	Protocol	Reference
10.7.1 Purchased software is used in accordance with contract agreements and copyright laws	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing audit and inventory processes and tools in use to detect improper use of software.	CMS

Guidance: A formal policy should be established regarding the use of purchased software. Related CSRs: 1.13.3

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

Control Technique	Protocol	Reference
10.7.2 Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the specified controls are in place and operating in accordance with the documented procedure. 3. Review documentation describing the software tracking system implemented to provide the specified controls.	CMS

Guidance: A formal program should be established with a policy and procedure. Related CSRs: 1.1.8, 6.5.2

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

Category: ***Network***

	General Requirement Control Technique	Protocol	Reference
10.7.3	A change-control mechanism that maintains control of changes to hardware, software, and security mechanisms is implemented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming use of the documented change-control mechanism. 3. Review documentation describing the change-control mechanism that is implemented to provide the specified controls.. 4. For a sample of hardware, software, and security mechanism, determine by inspection that the configuration of the sample item matches the documented baseline configuration for the item. 5. Compare sampled data, such as device type, serial number, and software version, from the current configuration management baseline system description with corresponding hardware, software, and security mechanism implementation to confirm precise match.	CMS

Guidance: A good approach might be to establish change control policies and procedures for all hardware, software, and security products.

Related CSRs: 5.9.3, 6.6.1, 3.4.1, 1.9.3, 6.1.2, 6.3.4

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

10.8 Logical Network Access Controls shall be in place.

	General Requirement Control Technique	Protocol	Reference
10.8.1	Any connection to the internet, or other external networks or systems, occurs through a gateway/firewall.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing controls implemented to insure compliance with this requirement.	CMS FISCAM IRS 1075

Guidance: A firewall must separate corporate computers and servers from the internet or other external networks or systems. Workstations and servers behind the corporate firewall must not have a modem connection. Modem connections will be handled via an authorized dial-in server.

Related CSRs:

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

	General Requirement Control Technique	Protocol	Reference
10.8.2	Authentication is used to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; (3) grant access to the functions of critical network devices; (4) procedures for the above are documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of all required authentication functions.	CMS HIPAA

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

Related CSRs: 2.9.6, 2.9.5

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

Category: ***Network***

General Requirement Control Technique	Protocol	Reference

10.8.3 The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored.

1. Review relevant policies and procedures for inclusion and directed use of the required process and specification of the warning message(s) to be used.
2. View the required warning message displayed on the opening screen seen by system users each type of server, workstation, and terminal used in the system.
3. For a sample, including each type of network device supporting the feature, view the required warning message displayed on the opening screen seen by anyone attempting to directly access the device from the network or console.

FISCAM

Guidance: The choice of which screen warning banner to implement is up to the system owner and should be based on system-specific technology limitations, data sensitivity, or other unique system requirements.

Related CSRs: 2.8.7

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

10.8.4 Workstation with dial-up access generate a unique identifier code before connection is completed.

1. Review documented dial-up procedure to confirm inclusion of the required features.
2. Observe a sample of dial-up connections involving each type of access controller.

FISCAM

Guidance: If workstations have dial-up access, ensure that a unique ID code is generated for each dial-up session.

Related CSRs:

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

10.9 Vulnerabilities to physical and cyber attacks shall be assessed.

10.9.1 A plan is in place to assess the risks to the network.

Review the required plan and approved implementing instructions.

PDD 63

Guidance: A formal program is in place for determining when and how to assess risks to the network.

Related CSRs:

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

10.9.2 A plan is developed for eliminating significant vulnerabilities.

1. Review the required plan.
2. Review documentation establishing that the required plan eliminates all significant vulnerabilities.

PDD 63

Guidance: As part of the security management program, ensure that a plan is developed to minimize vulnerabilities.

Related CSRs:

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

10.9.3 A plan is developed for alerting, containing, and rebuffing a physical or cyber attack on the CMS Business Partner IS systems.

Review the required plan to confirm that it includes the specified features.

PDD 63

Guidance: A formal program should be established with documented policies and procedures.

Related CSRs:

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

10.9.4 Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming conduct of the required assessments at least annually.

PDD 63

Guidance: As part of the security management program, ensure that an annual assessment is performed.

Related CSRs: 1.9.8

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

10.10 Logical controls shall be implemented over telecommunications access.

	Control Technique	Protocol	Reference
10.10.1	Communication software has been implemented to verify workstation identifications in order to restrict access through specific workstations: (1) verify IDs and passwords for access to specific applications; (2) control access through connections between systems and workstations; (3) restrict an application's use of network facilities; (4) protect sensitive data during transmission; (5) automatically disconnect at the end of a session; (6) maintain network activity logs; (7) restrict access to table that define network options, resources, and operator profiles; (8) allow only authorized users to shutdown network components; (9) monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; (10) restrict in-house access to telecommunications software; (11) control changes to telecommunications software; (12) ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage and; (13) restrict and monitor access to telecommunications hardware or facilities.	1. Review documentation confirming implementation of communications software having all of the required features. 2. Review audit data confirming continuing operation of all specified features of the required software.	FISCAM

Guidance: Ensure that policies and procedures are in place that address all thirteen (13) of these points. If not, they should be developed in coordination with you company's IT department.

Related CSRs: 6.4.1, 2.9.6, 2.9.11, 2.8.4, 3.4.1, 2.9.8, 2.9.10, 3.6.2, 10.5.1

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