CMS Manual System

Pub 100-17 Medicare Business Partners Systems Security

Transmittal 7

Department of Health & Human Services (DHHS)

Centers for Medicare & Medicaid Services (CMS)

Date: MARCH 17, 2006

Change Request 4342

SUBJECT: Business Partner Systems Security Manual

I. SUMMARY OF CHANGES: Update to the Self-Assessment Process in Appendix A and the Core Security Requirements (CSRs) (Attachment A). The purpose of this update is to communicate to Medicare Contractors changes to the Self-Assessment process to incorporate the revision of NIST SP 800-26 (Rev 1) and update of the CSRs to include the requirements of NIST SP 800-53.

Appendix A is extensively reformatted; therefore, all the material is in red italics.

NEW/REVISED MATERIAL :

EFFECTIVE DATE : May 1, 2006

IMPLEMENTATION DATE : May 1, 2006

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

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

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

R/N/D	Chapter / Section / Subsection / Title
R	Appendix A
R	Attachment A

III. FUNDING:

No additional funding will be provided by CMS; Contractor activities are to be carried out within their FY 2006 operating budgets.

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

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

Attachment - Business Requirements

Pub. 100-17	**Transmittal: 7**	**Date: March 17, 2006**	**Change Request 4342**

SUBJECT: Business Partners Systems Security Manual

I. GENERAL INFORMATION

A. Background: This Change Request Updates the Self-Assessment Process in Appendix A and the Core Security Requirements (CSRs) (Attachment A). The purpose of this update is to communicate to Medicare Contractors changes to the Self-Assessment process to incorporate the revision of NIST SP 800-26 (Rev 1) and update of the CSRs to include the requirements of NIST SP 800-53.

B. Policy: The policy(s) mandating this change request are the Federal Information Security Management Act of 2002, National Institute of Standards and Technology guidance, and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS

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

Requirement Number	**Requirements**	**Responsibility (“X” indicates the columns that apply)**								
		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
4342.1	Medicare contractors shall follow the self-assessment process outlined in the Medicare Business Partners Systems Security Manual.	X	X	X	X	X	X	X	X	X (HIGLAS, MACs, EDCs & PCSs)
4342.2	Medicare Contractors shall follow the instructions and guidance when evaluating all CSRs and preparing CSR responses.	X	X	X	X	X	X	X	X	X (HIGLAS, MACs, EDCs & PCSs)

III. PROVIDER EDUCATION

Requirement Number	**Requirements**	**Responsibility (“X” indicates the columns that apply)**

		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
	None.									

IV. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions: N/A

X-Ref Requirement #	Instructions

B. Design Considerations: N/A

X-Ref Requirement #	Recommendation for Medicare System Requirements

C. Interfaces: N/A

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

E. Dependencies: N/A

F. Testing Considerations: N/A

V. SCHEDULE, CONTACTS, AND FUNDING

Effective Date*: May 1, 2006 **Implementation Date**: May 1, 2006 **Pre-Implementation Contact(s):** Kevin Potter 410.786.5685 and Sherwin Schulterbrandt 410.786.0743 **Post-Implementation Contact(s):** Kevin Potter 410.786.5685 and Sherwin Schulterbrandt 410.786.0743	**No additional funding will be provided by CMS; contractor activities are to be carried out within their FY 2006 operating budgets.**

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

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

Table of Contents

(Rev. 7, 03-17-06)

1.0 Introduction to the CMS Integrated Security Suite (CISS)

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

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

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

2.0 CISS Self-Assessment (CAST) Module

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

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

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

Business partners must complete the CISS Self-Assessment module and submit a copy on CD-ROM to both the CMS Central Office and the Consortium Contractor Management Officer (CCMO) for Title XVIII contracts or the Project Officer (PO) for Federal Acquisition Regulation (FAR) contracts by close of business April 28, 2006. Be advised that this information must not be submitted to the CMS via email. Registered mail or its equivalent should be used. Should you need technical assistance, contact the CMS/Northrop Grumman Help Desk at 703-620-8585.

The completed Self-Assessment must be included in the Security Profile (see section 3.7 of the BPSSM). Business partners may also use the CISS to conduct Self-Assessments in preparation for audits by specific external entities such as the Government Accounting Office (GAO), Internal Revenue Service (IRS), Department of Health and Human Services (DHHS) Office of Inspector General (OIG), and CMS. The CISS allows the Business Partner to generate a worksheet consisting of those CSRs and Protocols that have a particular source document as a reference (e.g., IRS Pub 1075, NIST, FISCAM, etc.).

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

2.1 Applicable Laws

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

CMS CSRs detail technical requirements for CMS Business Partners who use information 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 CMS CSRs are developed by assessing and analyzing requirement statements from a number of Federal and CMS mandates, including the following:

- *Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.* *http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html*
- *OMB Circular No. A-127, Financial Management Systems, June 21, 1995.*

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

  http://www.whitehouse.gov/omb/circulars/a127transmittal2.html
- *OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000.*

  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- *Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000.*

  http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html
- *Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources, December 17, 2003.*

  http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf
- *Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999.*

  http://www.gao.gov/special.pubs/12_19_6.pdf
- *NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.* *http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf*
- *CMS System Security Plans (SSP) Methodology, Draft Version 3.0, November 6, 2002.* *http://www.cms.hhs.gov/it/security/References/ps.asp*
- *CMS Information Security Risk Assessment Methodology, Version 2.1, April 22, 2005.* *http://www.cms.hhs.gov/it/security/References/ps.asp*

- *CMS Information Security Acceptable Risk Safeguards (ARS), Draft Version 2.2, July 20, 2005.*

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

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

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

- *Health Insurance Portability and Accountability Act (HIPAA), August 21, 1996.*

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

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

2.2 CSR Categories

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

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

Category	*Description*
Entity-wide Security Program Planning and Management	*These controls address the planning and management of an entity's control structure.*
Access Control	*These controls provide reasonable assurance that information-handling resources are protected against unauthorized loss, modification, disclosure, and damage. Access controls can be logical or physical.*
System Software	*These controls address access and modification of system software. System software is vulnerable to unauthorized change and this Category contains critical elements necessary for providing needed protection.*
Segregation of Duties	*These controls describe how work responsibilities are segregated so that one person does not have access to or control over all of the critical stages of an information handling process.*
Service Continuity	*These controls address the means by which the entity attempts to ensure continuity of service. A Business Partner cannot lose its capability to process, handle, and protect the information it is entrusted with.*
Application Software Development and Change Control	*These controls address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information (FTI).*
Application System Authorization Controls	*These controls address the processing of Medicare data in a manner that ensures that only authorized transactions are entered into the information processing system.*

Category	Description
Application System Completeness Controls	These controls ensure that all system transactions are processed and that any missing or duplicate transactions are identified and a remedy implemented.
Application System Accuracy Controls	These controls address the accuracy of all data entered into systems for processing, handing, and storage. Data must be valid and accurate. All invalid, erroneous, or inaccurate data must be identified and corrected.
Network	These controls address the network(s) structure. The network structure must be protected and the data transmitted on the networks must be protected.

Table A-1. CSR Category Descriptions

2.3 CSR Elements

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

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

<table>
<tr><td colspan="3"><b>Category:</b>
<b>1. Entitywide Security Program Planning and Management</b></td></tr>
<tr><td colspan="3"><b>General Requirement:</b>
1.1. Management and staff shall receive security training, security awareness, and have security expertise.</td></tr>
<tr><td rowspan="2">Control Technique:
1.1.1. Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).</td><td>Protocol(s):
1. Review the training policy.
2. Interview a sample of site personnel to verify that documented training was received.
3. Review documented procedure for generation of security reminders.
4. Review a sample of training records to confirm completion of the required training.
5. Review training syllabus for inclusion of the required training.</td><td>Reference(s):
NIST 800-53: AT-2
NIST 800-53: AT-3
HIPAA: 164.308(a)(5)(i)
HIPAA: 164.308(a)(5)(ii)(A)
HIPAA: 164.308(a)(5)(ii)(B)
HIPAA: 164.308(a)(5)(ii)(C)
HIPAA: 164.308(a)(5)(ii)(D)
ARS: AT-3.2
ARS: AT-2.3
FISCAM: TSP-4.2.2</td></tr>
<tr><td>Guidance:
A formal program should be established with a policy and a procedure.</td><td>Related CSR(s):
2.9.2, 5.12.1</td></tr>
<tr><td colspan="3">Applicable Types: COB, CWF, DC, Dmerc, PartA, PartB, PSC, SS, MAC</td></tr>
</table>

Table A-2. CSR Elements

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

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

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

- ***Protocols****. Recommended procedures designed to verify that a site is 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 CSRs. As such, they provide Business Partners with Self-Assessment procedures that are similar to audit procedures used by CMS and external agencies. This information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.*

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

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

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

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

Applicability legend:

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

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

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

- *Where Federal improvements are already covered by an existing CSR, these documents are added as references.*
- *Where Federal improvements are partially covered by an existing CSR, the existing CSR is modified to incorporate appropriate language and the appropriate document(s) are listed as reference(s).*
- *Where Federal improvements are not covered by an existing CSR, a new CSR is added and the appropriate document(s) are listed as a reference(s).*

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

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

2.4 Completing the Self-Assessment (CAST)

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

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

2.5 All Responses

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

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

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

b) Each CSR requires a Status (i.e., "Level 0," "Level 1," "Level 2," "Level 3," "Level 4," "Level 5," or "N/A") to be selected, and each CSR requires a detailed explanation in the Response Comment/Explanation field to describe and explain the compliance status. In addition, all CSR responses must include a complete description of What, Where, Why, and How each CSR is or is not in compliance, depending on the CSR status selection.

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

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

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

f) Each CSR in the CISS includes an Applicability matrix, which identifies the likely responsibility for each CSR by CMS contract type (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 to be used as a guide to Business Partners. CMS recognizes that system configurations vary widely throughout the Business Partner community; therefore, each Business Partner must evaluate and report on each CSR's applicability to its own systems.*

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

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

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

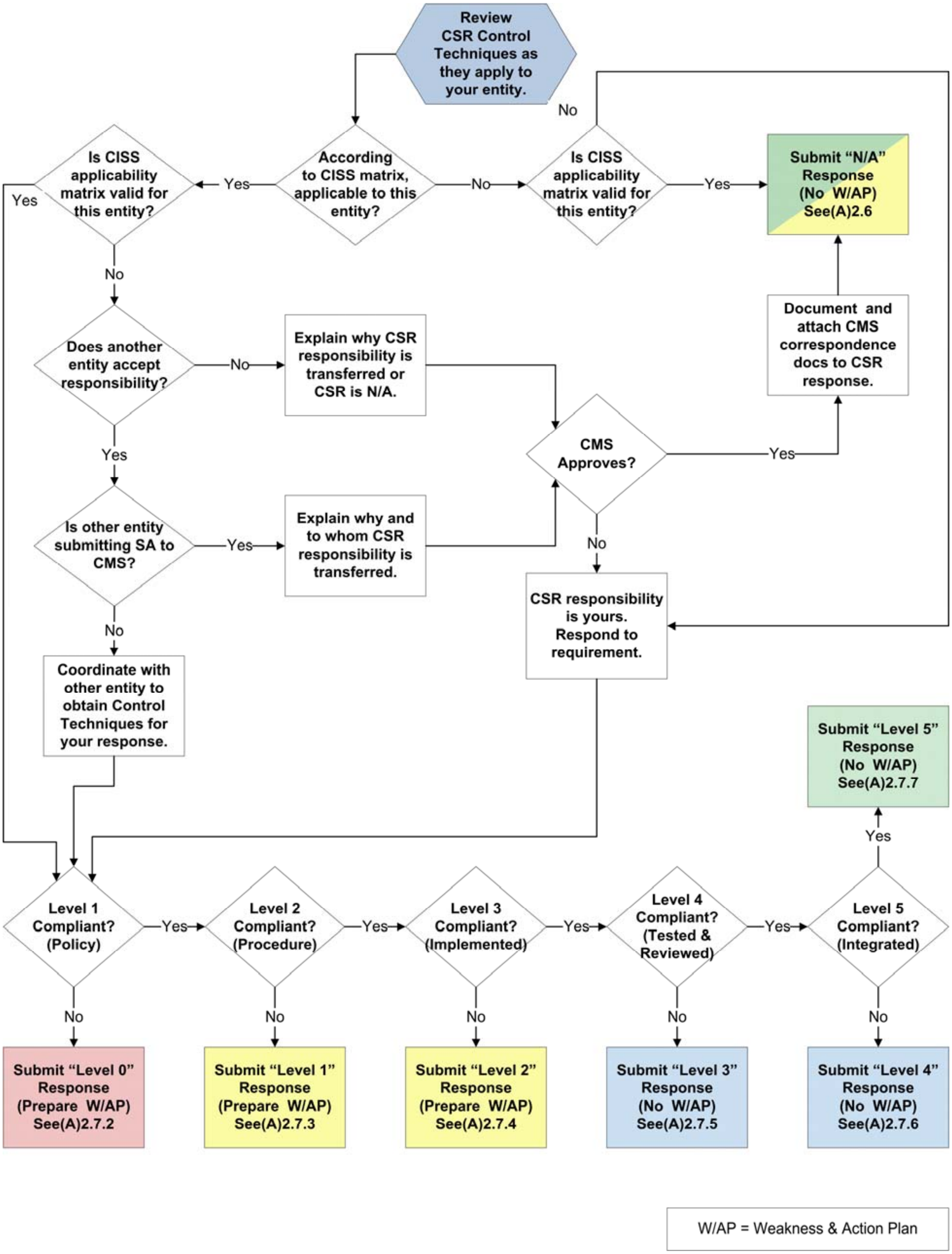
Review CSR Control Techniques as they apply to your entity.
According to CISS matrix, applicable to this entity?
Yes
No
Is CISS applicability matrix valid for this entity?
Yes
No
Is CISS applicability matrix valid for this entity?
No
Yes
Submit "N/A" Response (No W/AP) See(A)2.6
Does another entity accept responsibility?
No
Explain why CSR responsibility is transferred or CSR is N/A.
Yes
Document and attach CMS correspondence docs to CSR response.
CMS Approves?
Yes
No
Is other entity submitting SA to CMS?
Yes
Explain why and to whom CSR responsibility is transferred.
No
CSR responsibility is yours. Respond to requirement.
Coordinate with other entity to obtain Control Techniques for your response.
Submit "Level 5" Response (No W/AP) See(A)2.7.7
Yes
Level 1 Compliant? (Policy)
Yes
Level 2 Compliant? (Procedure)
Yes
Level 3 Compliant? (Implemented)
Yes
Level 4 Compliant? (Tested & Reviewed)
Yes
Level 5 Compliant? (Integrated)
No
No
No
No
No
Submit "Level 0" Response (Prepare W/AP) See(A)2.7.2
Submit "Level 1" Response (Prepare W/AP) See(A)2.7.3
Submit "Level 2" Response (Prepare W/AP) See(A)2.7.4
Submit "Level 3" Response (No W/AP) See(A)2.7.5
Submit "Level 4" Response (No W/AP) See(A)2.7.6
W/AP = Weakness & Action Plan

Figure A-1. Response Status Decision Tree

2.6 “N/A” Response Status

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

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

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

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

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

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

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

<u>The CISS tool will require that copies of the associated CMS approval documentation be attached to the CSR response within the CISS tool.</u> Approvals for prior years may be cited in your request for CMS approval for the current year response, but cannot be used as documentation of CMS approval for the current year CSR “N/A” response. Each year, the CMS approval process must be repeated (unless specifically stated in the CMS-provided approval documentation).

Include the following information with CMS-approved “N/A” responses, in addition to the requirements stated above in 2.6(a):

(1) Date CMS approved the response,

(2) CMS office that approved the response, and

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

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

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

2.7 Five Levels of Security Effectiveness

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

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

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

Table A-3. Levels of Security Effectiveness

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

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

b) ***Risk-Based Decision****. In some extreme cases, full implementation of the minimum compliance requirements may present unacceptable fiscal or configuration barriers. In these cases, CMS <u>may</u> agree that the risk is acceptable for the present self-assessment and that no Weakness/Action Plan combination is required nor desired. In such cases, <u>prior CMS concurrence is required</u> AND a full assessment of all of the implications of not meeting each of the minimum 3 levels for the applicable CSR is fully documented in the associated risk-assessment for the system. BOTH the updated risk-assessment AND full documentation of CMS concurrence MUST be attached to the CSR response.*

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

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

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

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

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

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

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

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

i. Do not include planned controls or controls that are not fully implemented. If all components are not fully in place, the response status must be changed to the next lower level and, if required, a suitable Weakness/Action Plan combination identified.

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

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

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

2.7.2 "Level 0" Response Status

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

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

2.7.3 "Level 1" Response Status

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

Level 1 – Policy – includes:

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

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

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

2.7.4 "Level 2" Response Status

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

Level 2 – Procedures – includes:

- *Formal, complete, well-documented procedures for implementing policies established at Level 1.*
- *The basic requirements and guidance issued from applicable public laws; other Federal, department, and agency policy; as well as applicable NIST publications.*

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

2.7.5 "Level 3" Response Status

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

Level 3 – Implemented – includes:

- *Security procedures and controls that are implemented.*
- *Procedures that are communicated and individuals are required to follow them.*

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

2.7.6 "Level 4" Response Status

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

Level 4 – Tested – includes:

- *Routinely evaluating the adequacy and effectiveness of security policies, procedures, and controls.*
- *Ensuring that effective corrective actions are taken to address identified Weaknesses, including those identified as a result of potential or actual security incidents or through security alerts issued by Federal organizations, vendors, and other trusted sources.*

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

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

To be effective, routine assessments must include tests and examinations of security controls. Reviews of documentation, walk-through of Business Partner facilities, and interviews with Business Partner personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. To be meaningful, assessments should include security controls of interconnected assets (e.g., network supporting applications being tested).

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

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

2.7.7 "Level 5" Response Status

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

Level 5 – Integrated – includes:

- *A comprehensive security program that is an integral part of a Business Partner's organizational culture.*
- *Decision-making based on cost, risk, and mission impact.*

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

- *Improving security program,*
- *Improving security program procedures,*
- *Improving or refining security controls,*
- *Integrating security within existing and evolving IT architecture, and*
- *Improving mission processes and risk management activities.*

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

2.8 Findings and Weaknesses

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

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

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

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

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

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

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

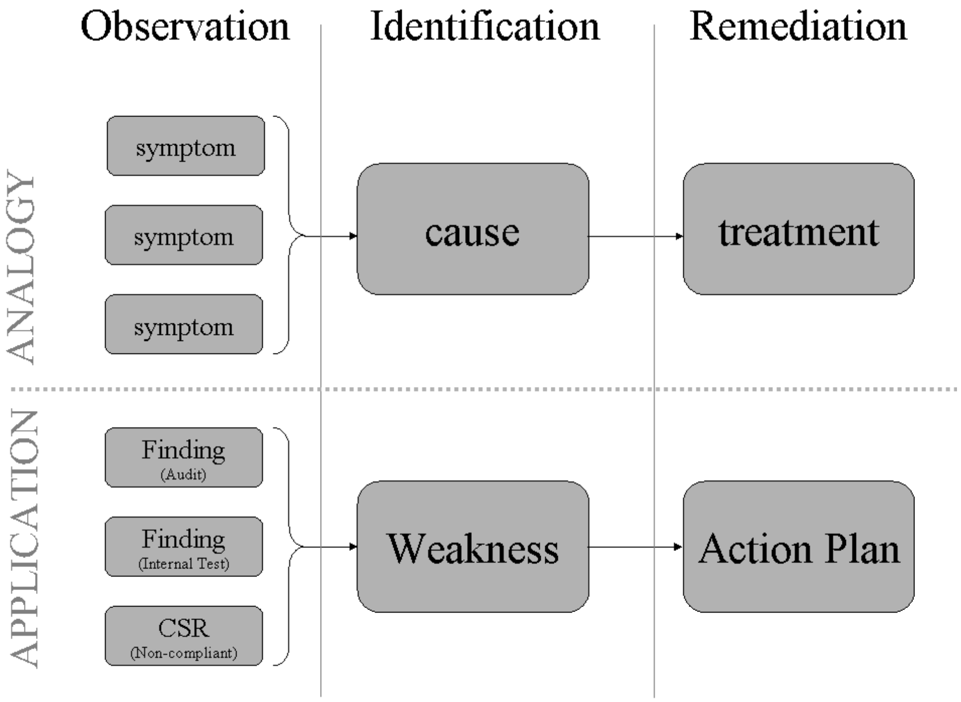

Figure A-2. Analogy for Finding-Weakness-Action Plan Relationship

An Action Plan must be designated to address each Weakness.

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

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

- *Risk assessments*
- *Internal or self-directed reviews, audits, or tests.*

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

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

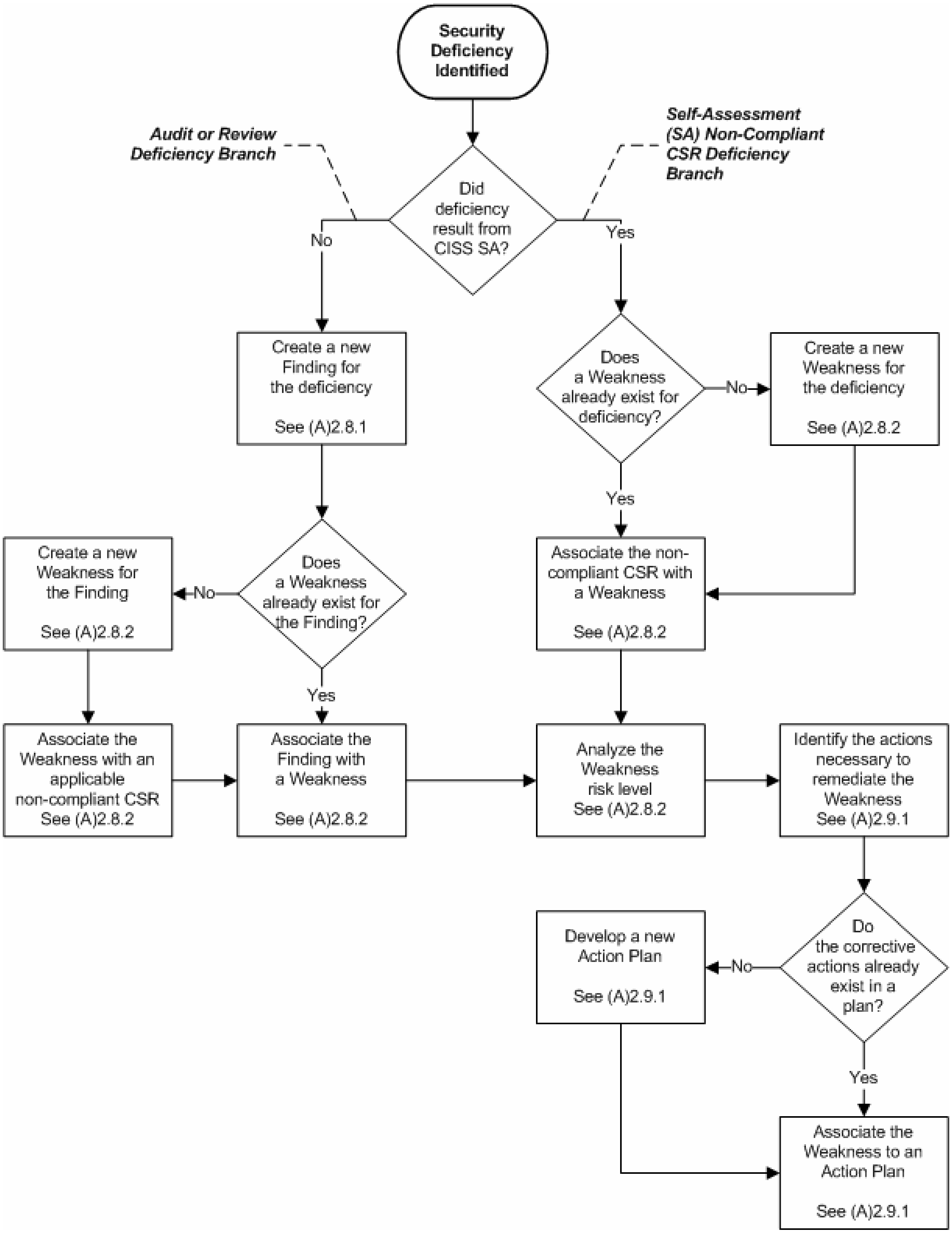
Security Deficiency Identified
Audit or Review Deficiency Branch
Self-Assessment (SA) Non-Compliant CSR Deficiency Branch
Did deficiency result from CISS SA?
No
Yes
Create a new Finding for the deficiency
See (A)2.8.1
Does a Weakness already exist for deficiency?
No
Create a new Weakness for the deficiency
See (A)2.8.2
Yes
Associate the non-compliant CSR with a Weakness
See (A)2.8.2
Create a new Weakness for the Finding
See (A)2.8.2
No
Does a Weakness already exist for the Finding?
Yes
Associate the Weakness with an applicable non-compliant CSR
See (A)2.8.2
Associate the Finding with a Weakness
See (A)2.8.2
Analyze the Weakness risk level
See (A)2.8.2
Identify the actions necessary to remediate the Weakness
See (A)2.9.1
Develop a new Action Plan
See (A)2.9.1
No
Do the corrective actions already exist in a plan?
Yes
Associate the Weakness to an Action Plan
See (A)2.9.1

Figure A-3. Weakness Decision Tree

2.8.1 Findings

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

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

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

2.8.1.1 Finding Identifier

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

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

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

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

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

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

- *R - Accounts Receivable review*
- *C - CPIC, (your annual self certification package)*
- *E - CFO EDP review*
- *F - CFO Financial review*
- *S - Statement on Auditing Standards no. 70 (SAS 70)*
- *O - OIG reviews (HHS Office of Inspector General [Information Technology] controls assessment)*
- *G - GAO reviews (financial reviews)*
- *P - CMS 1522 workgroups reviews*
- *V - CFO related NVA/ST*
- *N - SAS 70 Novation;*
- *M - CMS CPIC workgroup reviews*
- *9T - Section 912 Testing*

- *9E - Section 912 Evaluations*
- *AC - CMS self-assessment Annual Compliance Audits*
- *IR - Internal reviews initiated by the entity to meet other Federal requirements, and*
- *RA - Issues identified during routine risk assessments.*

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

2.8.1.2 Finding Title and Description
(Rev.7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

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

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

The Finding description should be the descriptive Finding information reported in the audit or review report. This description is not reported beyond CMS, so there is no restriction on its content. If the Finding is the result of an internal audit or review, the description should include the Finding information required by the GAO, "Government Auditing Standards," GAO-03-673G (http://www.gao.gov/govaud/yb2003.pdf), commonly referred to as the "Yellow Book."

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

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

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

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

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

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

2.8.1.4 Determination of Finding Risk Level
(Rev.7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)

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

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

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

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

- *A **Reportable Condition** exists when the internal controls are adequate in design and operation and reasonable assurance can be provided that the intent of the control objective is met, but deficiencies were found during the review that require correction.*

- *A **Material Weakness** exists when the Business Partner fails to meet a control objective. This may be due to a significant deficiency in the design and/or operation of internal control policies and procedures. Because of these shortfalls in internal controls, the Business Partner cannot provide reasonable assurance that the intent of the control objective is being met.*

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

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

- *Risk Management*

- *Review of Security Controls*
- *Life Cycle*
- *Authorized Processing (C&A)*
- *Systems Security Plan*
- *Personnel Security*
- *Physical Security*
- *Production I/O Controls*
- *Contingency Planning*
- *H/W and Systems Maintenance*
- *Data Integrity*
- *Documentation*
- *Security Awareness, Training, and Education*
- *Incident Response Capability*
- *Identification and Authentication*
- *Logical Access Controls*
- *Audit Trails*

2.8.1.7 Finding Point(s) of Contact

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

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

2.8.2 Weaknesses

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

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

Weaknesses resulting from Self-Assessment non-compliant CSRs (i.e., a response status other than "Level 3," "Level 4," "Level 5," or "N/A") may also be associated with (i.e., linked to) existing Findings but normally are not associated with Findings. Weaknesses derived from a non-compliant CSR do not require an association to a Finding. However, ALL Weaknesses MUST be associated with AT LEAST ONE non-compliant CSR.

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

2.8.2.1 Weakness Identifier

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

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

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

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

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

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

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

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

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

2.8.2.2 Weakness Title and Description

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

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

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

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

2.8.2.3 Weakness Category

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

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

- *Risk Management*
- *Review of Security Controls*
- *Life Cycle*
- *Authorized Processing (C&A)*
- *System Security Plan*
- *Personnel Security*
- *Physical Security*
- *Production I/O Controls*
- *Contingency Planning*
- *H/W and Systems Maintenance*
- *Data Integrity*
- *Documentation*
- *Security Awareness, Training, and Education*
- *Incident Response Capability*
- *Identification and Authentication*
- *Logical Access Controls*
- *Audit Trails.*

2.8.2.4 Determination of Weakness Risk Level

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

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

2.8.2.5 Weakness FISMA Severity

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

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

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

The three FISMA Severity levels are:

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

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

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

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

2.8.2.6 Weakness Type

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

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

- ***Program Weakness**. A Program Weakness impacts multiple IT systems as a result of a deficiency in the IT security program.*
- ***System Weakness**. A System Weakness pertains to the management, operation, or technical controls of a specific IT system.*

2.8.2.7 Weakness Status

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

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

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

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

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

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

2.8.2.8 Weakness Point(s) of Contact

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

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

2.8.2.9 Determining Risk

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

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

While both system and business risk measurements are discussed and combined in the CMS RA Methodology document, risk determinations made in and by the CISS are for systems only. The system risk level is derived by combining the threat likelihood value and threat impact value for a specific threat/vulnerability pair, as follows:

1. ***Determine Likelihood***. *Determine the likelihood of an identified system threat exploiting a specific identified vulnerability.*

2. ***Determine Impact***. *Determine the impact that such an exploitation would have on the system's operation and information.*

3. ***Determine Risk***. *Determine the overall risk using the values derived in steps 1 and 2 above. This step is completely automatically by the CISS.*

2.8.2.9.1 Likelihood

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

The risk likelihood level is determined by considering known threats as they may apply to known system vulnerabilities. The likelihood that a vulnerability will be exploited by a threat is assessed and described as High, Medium, or Low. Factors that govern the likelihood of vulnerability exploitation include threat capability, frequency of threat occurrence, and effectiveness of current countermeasures. The descriptions provided in A-4 should be used to determine the likelihood level for a threat/vulnerability pair.

Likelihood Levels	***Likelihood Definition***
High	*The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.*
Medium	*The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.*
Low	*The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.*

Table A-4. Likelihood Levels

2.8.2.9.2 Impact

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

Risk impact refers to the magnitude of harm that may result from the exploitation of a given threat/vulnerability pair. Impact is determined by the value of the resources at risk, both in terms of its inherent (i.e., replacement) value and its importance (i.e., criticality) to CMS' mission. The criticality and sensitivity of both the system and data are useful guides for assessing the potential impact of an exploited vulnerability. The descriptions provided in Table A-5 should be used to determine the level of impact.

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

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

Table A-5. Magnitude of Impact Definitions

2.8.2.9.3 Overall Risk

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

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

Threat Likelihood	Impact		
	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Table A-6. Overall Risk Matrix

2.9 Action Plans and POA&Ms

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

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

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

2.9.1 Completing Action Plans

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

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

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

2.9.1.1 Action Plan Title and Description

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

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

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

2.9.1.2 Determining Completion Dates

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

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

2.9.1.3 Determining Costs

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

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

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

- *Risk assessment*
- *Security planning and policy*
- *Certification and accreditation*
- *Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)*
- *Authentication or cryptographic applications*

- *Education, awareness, and training*
- *System reviews/evaluations (including security control testing and evaluation)*
- *Oversight or compliance inspections*
- *Development and maintenance of Business Partner reports to CMS and corrective Action Plans as they pertain to the specific investment*
- *Contingency planning and testing*
- *Physical and environmental controls for hardware and software*
- *Auditing and monitoring*
- *Computer security investigations and forensics*
- *Reviews, inspections, audits, and other evaluations performed on Business Partner facilities and operations.*

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

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

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

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

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

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

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

2.9.1.4 Determining Funding Sources

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

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

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

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

2.9.1.5 Milestone Title and Description

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

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

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

2.9.1.6 Milestones with Completion Dates

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

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

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

The overall projected completing date of the Action Plan is derived automatically by the CISS based on the projected completion dates of all of the Milestones. The Initial Target date remains *unchanged one the Action plan has been submitted to CMS. However, the Current Projected Date will adjust automatically based on changes in milestone projected completion date. (Note that the Action Plan status of "Delayed" is always calculated based on the Initial Target date.)*

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

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

2.9.1.7 Milestone Changes

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

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

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

1. *Entitywide Security Program Planning and Management*

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

General Requirement Control Technique	Protocol	Reference
1.1.1 Security training includes the following topics and related procedures: (1) awareness training; (2) periodic security reminders (e.g., posters, booklets); (3) user education concerning malicious software; (4) user education in importance of monitoring login success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed when creating and changing passwords, and the need to keep them confidential).	1. Review training syllabus for inclusion of the required training. 2. Review a sample of training records to confirm completion of the required training. 3. Review documented procedure for generation of security reminders. 4. Review the training policy. 5. Interview a sample of site personnel to verify that documented training was received.	PISP 4.2.9.2 PISP 4.2.9.3 HIPAA 164.308(a)(5)(i) HIPAA 164.308(a)(5)(ii)(A) HIPAA 164.308(a)(5)(ii)(B) HIPAA 164.308(a)(5)(ii)(C) HIPAA 164.308(a)(5)(ii)(D) FISCAM TSP-4.2.2 NIST 800-53 AT-2 NIST 800-53 AT-3 ARS AT-2.CMS-1 ARS AT-3.0
Guidance: A formal program should be established with a policy and a procedure.		Related CSRs: 5.12.1, 2.9.9, 2.9.7
☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.1.2 All information system users (i.e., employees, including managers and senior executives, 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.	PISP 4.2.9.2 FISCAM TSP-3.3.1 IRS 1075 6.2@1.1 CMS Directed HIPAA 164.308(a)(5)(i) IRS 1075 6.2@1.3 IRS 1075 6.2@1.4 IRS 1075 6.2@1.2 NIST 800-53 AT-2 NIST 800-53 AT-3 ARS AT-2.0 ARS AT-3.0 PISP 4.2.9.3
Guidance: Security awareness and security training should inform personnel, including contractors and other users of information systems that support Medicare claims processing of: (1) the proper rules of behavior while using Medicare claims processing systems and information, and (2) their responsibilities in complying with security policies and procedures. Security awareness and security training is provided before allowing access to any sensitive information or system. Security awareness should be a continuing effort but it should be repeated, minimally, on an annual basis.		Related CSRs: 1.10.1, 2.9.6, 1.4.1
☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.1.3 Security training is provided upon employment, promotion, and is adjusted or customized based on the level of the employee's role and responsibilities (i.e., the necessary security skills and competencies necessary to perform a specific role and responsibility).	For a sample of personnel, review training documentation and job descriptions for evidence of customization of security training to the level of job responsibilities.	CMS Directed NIST 800-53 AT-2 NIST 800-53 AT-3 PISP 4.2.9.3 PISP 4.2.9.2
Guidance: Security training for an SSO or system security administrator requires more in-depth security skills and competencies (e.g., security controls, incident response, vulnerabilities, etc.) than a claims entry clerk who only requires basic security training on the proper use of security in relation to the processing of sensitive data (e.g., rules of behavior).		Related CSRs: 3.2.1, 3.2.2
☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

1.1.4 The employees acknowledge, in writing or electronically, having received the security and awareness training. A record of the security awareness and security training subject(s) covered is maintained.

1. Verify that records are being maintained that document the security awareness and security training subjects covered.
2. Verify that records show all employees have acknowledged receiving security and awareness training.
3. Check a random sample of employee records to verify training attendance signatures or electronic acknowledgment.

FISCAM TSP-4.2.3
CMS Directed
NIST 800-53 AT-4
PISP 4.2.9.4
ARS AT-4

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: 1.4.1

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

1.1.5 Security training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided. The use of peer-to-peer (P2P) file sharing technology is controlled and documented to ensure that P2P technology is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

Review documentation of policy and training to confirm the protection of copyright information under the terms of the provision of the copyright holder.

CMS Directed
NIST 800-53 SA-6
ARS SA-6
PISP 4.1.3.6

Guidance: A security policy should exist, and security training should include, appropriate information regarding copyright protection.

Related CSRs: 3.3.1, 7.1.3, 2.2.11, 10.7.1

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

1.1.6 System access is reviewed during extraordinary personnel circumstances.

1. Review relevant policies and procedures for inclusion of the required process.
2. Review the in-place controls for the individuals specified in this requirement.

ARS PS-CMS-1.CMS-1
PISP 4.2.1

Guidance: Screening should be consistent with the criteria established for the sensitivity designation of the assigned position.

Related CSRs: 1.10.1

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

1.1.7 Personnel with significant information security roles and responsibilities are required to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; and undergo refresher training annually thereafter.

For a sample of personnel, review training documentation and job descriptions for evidence of security training to the level of job roles and responsibilities.

PISP 4.2.9.3
NIST 800-53 AT-3
ARS AT-3.0

Guidance: The roles and responsibilities of an SSO or system security administrator require more in-depth security training and competencies (e.g., security controls, incident response, vulnerabilities, etc.) than a claims entry clerk who only requires basic security training on the proper use of security in relation to the processing of sensitive data (e.g., rules of behavior).

Related CSRs: 1.9.3

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

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

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

1. Records providing information on the monitoring activities should be available.
2. Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested.
3. Review logs and policy documentation to verify that security corrective actions have been monitored on a continuing basis.

FISCAM TSP-5.2
HIPAA 164.316(b)(2)(iii)

Guidance: A corrective security action would consist of designated safeguards from self-assessments, or similar items, developed as the result of an audit. Use of a designated manager, such as the SSO, to monitor implementation and to review the security configuration controls on a continuing basis would satisfy this requirement. This activity should be documented as an internal memorandum on an annual basis.

Related CSRs: 1.8.7, 1.12.3

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

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

	General Requirement Control Technique	Protocol	Reference
1.2.2	Budget requests (e.g., Line One funding, safeguards) include the allocation of security resources to adequately protect the system and include the determination of security requirements in mission/business planning.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review budget requests for inclusion of security resources necessary for the system.	NIST 800-53 SA-2 ARS SA-2 PISP 4.1.3.2

Guidance: The business partner includes the determination of security requirements for information systems in mission/business case planning and establishes a line item for information systems security in programming and budgeting documentation.

Related CSRs: 4.6.2

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

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

	General Requirement Control Technique	Protocol	Reference
1.3.1	Business Partners transmitting FTI from a main frame computer to another computer need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission. (This CSR applies only to the COB contractor.)	1. Review disclosure list for entries indicating that the documented process has been followed. 2. Interview responsible individual(s) to confirm understanding of the required procedure. 3. Review relevant policies and procedures for inclusion of the required logging process elements. 4. For a sample of documents being received from the IRS, observe handling of receipt of sensitive information for compliance with established procedures.	IRS 1075 3.3@2.2

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

Related CSRs: 1.3.8

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

	General Requirement Control Technique	Protocol	Reference
1.3.2	Sensitive information, other than that on magnetic tape files or disclosed as a function of normal claims processing operations (e.g., system processes, mailings, payments, etc.), disclosed outside the CMS Business Partner is recorded on a separate list that includes: (1) to whom the disclosure was made; (2) what was disclosed; (3) why it was disclosed; and (4) when it was disclosed.	1. Observe transmittal of sensitive information for compliance with established procedures. 2. Review relevant policies and procedures for inclusion of the required logging process elements. 3. Review disclosure list for entries indicating that the documented process has been followed. 4. Interview responsible individual(s) to confirm understanding of the required procedure.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(I) IRS 1075 3.3@2.1 HIPAA 164.312(c)(1) HIPAA 164.528(b)(2)

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, 1.4.2

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

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

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

CMS Directed
HIPAA 164.310(d)(2)(iii)
NIST 800-53 MP-2
NIST 800-53 MP-5
ARS MP-5
HIPAA 164.310(d)(1)
PISP 4.2.7.2
PISP 4.2.7.5

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: 2.2.26, 2.2.25

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

1.3.4 All retired, discarded, or unneeded sensitive data is disposed of in a manner that prevents unauthorized persons from using it. All sensitive data is cleared from storage media before releasing as work tapes or disks. Any magnetic media, compact disk, or hard drive that can not be sanitized for reuse is destroyed. Ensure the destruction of any sensitive information hard copy documents when no longer needed.

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

HIPAA 164.312(c)(2)
IRS 1075 6.3@7
HIPAA 164.312(e)(2)(i)
CMS Directed
HIPAA 164.310(d)(2)(i)
HIPAA 164.310(d)(2)(ii)
HIPAA 164.312(c)(1)
NIST 800-53 MP-7
ARS MP-7.CMS-1
PISP 4.2.7.7

Guidance: A good approach assures policies and procedures exist for release and/or destruction of CMS sensitive information. A record should be maintained that verifies who performed the destruction and when sensitive information was destroyed.

Related CSRs: 5.9.11, 5.9.12, 5.9.14

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

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

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

HIPAA 164.316(b)(2)(i)
CMS Directed

Guidance: Review retention procedures in relation to CMS PMs. When utilizing commercial storage facilities for off-site storage, ensure that any agreements in place address these Federal standards.

Related CSRs: 1.7.1

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

	General Requirement Control Technique	Protocol	Reference
1.3.6	Sensitive information is never disclosed during disposal unless authorized by statute. Destruction of sensitive information is witnessed by a CMS Business Partner employee. However, a Business Partner may elect to have the destruction certified by a shredding contractor in the absence of Business Partner participation.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review a sample of destruction records to confirm consistent use of the procedure.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) IRS 1075 8.4@1.5 HIPAA 164.308(a)(4)(i) HIPAA 164.310(d)(2)(ii) HIPAA 164.310(d)(2)(iii) IRS 1075 8.4@1.1 HIPAA 164.312(c)(1) IRS 1075 8.4@1.4 IRS 1075 8.4@1.3 IRS 1075 8.4@1.2 IRS 1075 8.4@1.6

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: 1.11.1

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

1.3.7	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. The sanitization process shall include the removal of all data, labels, marking, and activity logs. Procedures are in place to clear sensitive information and software from computers, memory areas, disks, and other equipment or media before they are disposed of or transferred to another use. The responsibility for clearing information is clearly assigned, and standard forms or a log is used to document that all discarded or transferred items are examined for sensitive information and this information is cleared before the items are released.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming consistent use of the required procedure.	HIPAA 164.312(c)(2) HIPAA 164.312(e)(2)(i) HIPAA 164.310(d)(2)(i) HIPAA 164.310(d)(2)(ii) IRS 1075 5.3@2.3 FISCAM TAC-3.4 HIPAA 164.312(c)(1) NIST 800-53 MA-3 NIST 800-53 MP-6 ARS MA-3.3 ARS MP-6.0 HIPAA 164.310(d)(1) PISP 4.2.5.3 PISP 4.2.7.6

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

Related CSRs: 2.12.2, 2.14.1

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

1.3.8	Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. FTI is physically destroyed by authorized personnel, or returned to the originator or to the system security administrator. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)	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 procedure.	IRS 1075 8.1 IRS 1075 6.3@6.1 IRS 1075 6.3@6.2

Guidance: A formal security program should be established with a policy and procedure. A good approach when returning FTI information to CMS is to obtain a receipt, and provide a notification which contains when and why the information was obtained, how long and for what reason(s) it was used, and when it was returned so as to make the FTI information usage traceable.

Related CSRs: 1.3.1

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

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

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

HIPAA 164.312(c)(2)
HIPAA 164.312(e)(2)(i)
HIPAA 164.312(c)(1)
NIST 800-53 MP-7
ARS MP-7.CMS-2
PISP 4.2.7.7

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

Related CSRs:

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

1.3.10 Inventory records of all storage media containing sensitive data must be maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media will be recorded in a log that identifies: (1) date received, (2) reel/cartridge control number contents, (3) number of records if available, (4) movement, and (5) if disposed of, the date and method of destruction. Such a log must permit all storage media containing sensitive data (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and logged.

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

HIPAA 164.312(c)(2)
HIPAA 164.312(e)(2)(i)
HIPAA 164.310(d)(2)(iii)
IRS 1075 4.6@3.1
HIPAA 164.312(c)(1)
FISCAM TAC-3.1.A.6
CMS Directed
IRS 1075 3.2@1.3
IRS 1075 3.2@2.2
NIST 800-53 MP-2
NIST 800-53 MP-3
NIST 800-53 MP-5
ARS MP-3.CMS-1
ARS MP-5
ARS MP-CMS-1.CMS-1
NIST 800-53 MP-8
PISP 4.2.7.2
PISP 4.2.7.3
PISP 4.2.7.5
PISP 4.2.7

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: 1.5.6, 5.4.6

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

1.3.11 Semiannual inventories of removable storage devices and media containing sensitive information are performed.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.

IRS 1075 3.2@2.3

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: 6.6.1

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

1.3.12 Removable storage devices and media containing sensitive information are secured before, during, and after processing, and a proper acknowledgement form is signed and returned to the originator.

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

IRS 1075 3.2@1.1

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

Related CSRs: 2.2.20

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

1.3.13 Whenever possible computer operations are in a secure area with restricted access. Sensitive information is kept locked when not in use. Tape reels, disks, or other media are labeled as CMS Sensitive Information. Any magnetic media or compact disk containing sensitive data is kept in a secured area. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming location of computer operations are in a secure area with restricted access, or that establishes approved use of equivalent safeguards.

HIPAA 164.312(c)(2)
HIPAA 164.312(e)(2)(i)
HIPAA 164.310(a)(1)
HIPAA 164.310(c)
IRS 1075 4.6@1.2
IRS 1075 4.6@1.5
HIPAA 164.312(c)(1)
CMS Directed
NIST 800-53 MP-3
NIST 800-53 MP-4
ARS MP-3.0
ARS MP-4.CMS-3

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: 2.2.3, 2.5.5

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

1.4 Owners and users shall be aware of security policies.

1.4.1 Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; (6) assuring that system users, including maintenance personnel, receive security awareness training; (7) implementing procedures to determine that the access of a workforce member to CMS sensitive information is appropriate; and (8) establishing a process for requesting, establishing, issuing, and closing user accounts.

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

HIPAA 164.308(a)(3)(i)
HIPAA 164.308(a)(3)(ii)(A)
HIPAA 164.308(a)(3)(ii)(B)
PISP 4.2.1.5
NIST 800-53 IA-4
NIST 800-53 PS-5

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

Related CSRs: 4.2.1, 1.8.2, 2.2.31, 3.5.2, 2.8.6, 2.8.2, 5.9.9, 1.10.2, 1.1.2, 1.1.4

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

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

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

IRS 1075 10.1
HIPAA 164.308(a)(6)(ii)
FISCAM TAC-4.3.3

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

Related CSRs: 1.3.2, 1.11.1, 2.1.9, 10.3.3

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

	General Requirement Control Technique	Protocol	Reference
1.4.3	Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; (3) rules that describe expected behavior of all with access to the system; and (4) procedures to prevent, detect, contain, and correct security violations. Employees acknowledge availability of these policies in writing or electronically.	1. Review policies and procedures for the required distribution process(es). 2. Review the distributed security policies for inclusion of the required rules. 3. Interview a sample of site personnel to verify that security policies are distributed.	FISCAM TSP-3.3.2 HIPAA 164.308(a)(1)(i) NIST 800-53 PL-4 NIST 800-53 PS-6 ARS PL-4.CMS-2 ARS PS-6 PISP 4.1.2.4 PISP 4.2.1.6

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: 6.4.2, 6.3.7, 9.6.1, 1.5.1, 1.9.1

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

1.4.4	Procedures are implemented for employees to follow when they discover a privacy breach or a violation of IS systems security. The procedures stipulate: (1) what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.	Review relevant policies and procedures for inclusion and directed use of the required procedures.	CMS Directed HIPAA 164.308(a)(6)(i) HIPAA 164.308(a)(6)(ii) NIST 800-53 IR-2 HSPD-7 H(25)(b) ARS IR-2.0 PISP 4.2.8.2

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

Related CSRs: 1.6.3, 1.6.1, 1.6.2, 1.6.5, 10.9.1, 10.9.2

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

1.4.5	Employees are made aware that company policy prohibits the browsing of sensitive data files for any reason other than Medicare business. Medicare information is not used in the CMS Business Partner's private line of business unless authorized by CMS as consistent with the Privacy Act.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm awareness of, and adherence to this policy.	CMS Directed

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

Related CSRs: 2.9.1, 10.3.4

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

1.4.6	Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information. Notify users that: (1) they are accessing a U.S. Government information system; (2) CMS maintains ownership and responsibility for its computer systems; (3) users must adhere to CMS Information Security Policies, Standards, and Procedures; (4) user's usage may be monitored, recorded, and audited; (5) unauthorized use is prohibited and subject to criminal and civil penalties; and (6) the use of the information system establishes user's consent to any and all monitoring and recording of their activities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample representing each type of computer operating system, and for standalone and each mode of network connection affecting banner display, observe that the warning banner on the sample computer is consistent with the documented procedure.	IRS 1075 5.1@1.3 CMS Directed NIST 800-53 AC-8 ARS AC-8.CMS-1 PISP 4.3.2.8

Guidance: The log-on banner/screen warning banner warns the user that the system processes sensitive information and it is subject to monitoring each time they log-on.

Related CSRs: 10.8.3, 10.6.2, 1.4.8

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

1.4.7	All warning banners were developed and implemented in conjunction with legal counsel. The warning message is displayed on the user's screen until the user takes explicit actions to log-on to the information system or cancel the session.	1. Examine the information system warning banner. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 AC-8 ARS AC-8.CMS-5 ARS AC-8.CMS-3 ARS AC-8.CMS-2 PISP 4.3.2.8

Guidance: Policies and procedures should exist for developing and implementing warning banners.

Related CSRs: 10.8.3

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

1.4.8	If keystroke monitoring is used, users are notified.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 AC-8 ARS AC-8.CMS-1 PISP 4.3.2.8

Guidance: Establish a policy and procedures on the use and control of keystroke monitoring.

Related CSRs: 1.4.6, 3.2.2

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

1.5 Information security responsibilities shall be clearly assigned.

	Control Technique	Protocol	Reference
1.5.1	The system security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security roles, responsibilities, and expectations for system and network use are clearly defined for: (1) information resource owners and users; (2) information resources management and data processing personnel; (3) senior management; and (4) security administrators.	1. Review the security plan for inclusion of the required identification of ownership of each computer-related resource, and of responsibilities for managing access to each of these resources. 2. Review the security plan for inclusion of definition of security responsibilities and expected behavior for at least each of the four specified categories of personnel.	FISCAM TSP-3.2 NIST 800-53 PL-4 NIST 800-53 PS-6 ARS PL-4.CMS-1 PISP 4.1.2.4 PISP 4.2.1.6

Guidance: Ensure that the Rules of Behavior are contained in the SSP and that they clearly define the responsibility of all employees. Related CSRs: 1.4.3, 4.7.3

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

	Control Technique	Protocol	Reference
1.5.2	The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.	Review documentation verifying that an SSO with the required qualifications is designated at an overall level, and at any subordinate levels designated as appropriate by the Business Partner.	FISCAM TSP-3.1.2 CMS Directed HIPAA 164.308(a)(2) ARS PS-CMS-2.CMS-1 PISP 4.2.1

Guidance: An approach is to certify or ascertain that the SSO has a CISA, CISSP or other appropriate information security certification. Related CSRs: 9.6.4, 9.6.6, 9.6.3

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

	Control Technique	Protocol	Reference
1.5.3	The SSO is organizationally independent of IS operations. If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.	1. If these additional SSO positions exist, review documentation supporting use of the specified process. 2. Review documentation supporting the required organizational independence. 3. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed

Guidance: Ensure that the SSO's duties allow him/her to act independent of IS operations. Ensure that all Medicare related actions are cleared through the primary Medicare SSO. Related CSRs: 1.9.6

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

	Control Technique	Protocol	Reference
1.5.4	The SSO assures compliance with CMS systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with CMS systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by CMS Regional Officer and/or Consortium; (4) maintaining systems security documentation for review by CMS Regional Officer and/or Consortium; (5) consulting with the CCMO's designated security officer on systems security issues when there is a need for guidance or interpretation; (6) keeping up with new/advanced systems security technology; (7) participating in all planning groups, having the responsibility to subject all new systems/installations (and major changes) to the risk assessment process; and (8) making certain that specialists such as auditors, lawyers, and building engineers address security issues before changes are made.	1. Review documentation supporting SSO performance of each of the specified roles and responsibilities. 2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.	HIPAA 164.316(b)(2)(iii) CMS Directed ARS PS-CMS-2.CMS-1 PISP 4.2.1

Guidance: An approach is to include these in the SSO's job description. Related CSRs: 9.6.4, 3.1.2, 1.9.2

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

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

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

CMS Directed

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

Related CSRs: 6.3.3

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

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

Review documentation supporting designation of this responsibility to specific employees.

IRS 1075 3.2@1.2
FISCAM TAC-3.1.A.3
HIPAA 164.308(a)(2)
HIPAA 164.310(d)(1)

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

Related CSRs: 1.3.10, 2.2.20, 1.13.7

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

1.5.7 The SSO assures that: (1) internal controls are incorporated into new ADP information systems; (2) appropriate security controls with associated evaluation/test procedures are developed before any procurement action; (3) system security requirements and evaluation/test procedures are included in RFPs and subcontracts involving Medicare claims processing; and (4) requirements in solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

1. Review documentation supporting SSO performance of each of the specified roles and responsibilities.
2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.
3. Review contracts, RFPs, and other solicitation documentation for inclusion of the specified requirements.

HIPAA 164.308(b)(1)
HIPAA 164.308(b)(4)
HIPAA 164.314(a)(1)
NIST 800-53 SA-4
PISP 4.1.3.4

Guidance: NIST SP 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Related CSRs: 1.11.2

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

1.6 An incident response capability shall be implemented.

1.6.1 The following controls exist to identify and report incidents: (1) security incident procedures; (2) report procedures; (3) response procedures; (4) procedures to regularly review records of information system activity, such as security incident tracking reports; and (5) process to modify incident handling procedures and control techniques after an incident occurs. Automated mechanisms are employed to assist in the reporting of security incidents.

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

HIPAA 164.308(a)(1)(ii)(D)
HIPAA 164.308(a)(6)(i)
NIST 800-53 IR-6
ARS IR-6.1
HSPD-7 H(25)(b)
PISP 4.2.8.6

Guidance: Refer to sample procedures from the CERT website.

Related CSRs: 1.4.4, 1.9.3, 10.9.2

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

1.6.2 The CMS Business Partner's incident response capability has the following characteristics: (1) an understanding of the CMS Business Partners being served; (2) educated information owners and users that trust the incident handling team; (3) a means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; (5) links to other relevant groups; and (6) receipt and response to other pertinent security alerts/advisories. Automated mechanisms are employed to increase the availability of incident response-related information and support.

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

FISCAM TSP-3.4
NIST 800-53 IR-7
NIST 800-53 SI-5
ARS IR-7.1
PISP 4.2.8.7
PISP 4.2.6.5

Guidance: Refer to sample procedures from the CERT website.

Related CSRs: 1.4.4, 1.9.3, 10.9.2

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

	General Requirement Control Technique	Protocol	Reference
1.6.3	Relevant security incident information is documented according to CMS Computer Security Incident Handling Procedures. Evidence is preserved through technical means, including secured storage of evidence media and write-protection of evidence media. Sound forensics processes are used in addition to utilities that support legal requirements means. The appropriate chain of custody is determined and followed for forensic evidence once an incident has occurred.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Interview response team personnel. 3. Examine secure storage area.	NIST 800-53 IR-4 ARS IR-4.CMS-2 ARS IR-4.CMS-1 PISP 4.2.8.4

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Related CSRs: 1.4.4, 1.9.3

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

1.6.4	The incident response capability includes: (1) providing refresher training on incident response roles and responsibilities of personnel on an annual basis; (2) incorporating simulated events as part of incident response training; and (3) employing automated mechanisms to provide a more thorough and realistic incident response training environment.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Interview response team personnel.	NIST 800-53 IR-2 ARS IR-2.1 ARS IR-2.2 ARS IR-2.0 PISP 4.2.8.2

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Related CSRs: 1.9.3, 5.6.2

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

1.6.5	Security incidents are tracked and documented on an on-going basis. Automated mechanisms are employed to assist in tracking and analyzing security incidents. The incident response capability is tested and documented annually, using reviews, analyses, and simulations. Automated mechanisms are employed to test the incident response plan.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Interview response team personnel.	NIST 800-53 IR-3 NIST 800-53 IR-5 ARS IR-3.1 ARS IR-3.0 ARS IR-5.1 PISP 4.2.8.3 PISP 4.2.8.5

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Related CSRs: 1.4.4

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

1.6.6	Vulnerabilities exploited during a security incident are identified, and security safeguards are implemented to reduce risk and vulnerability exploit exposure, including isolation or system disconnect. Automated mechanisms are employed to support the incident handling process.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Interview response team personnel.	NIST 800-53 IR-4 ARS IR-4.CMS-3 ARS IR-4.1 PISP 4.2.8.4

Guidance: Carefully constructed procedures should be in place for protecting forensic evidence and documenting security incident-related information.

Related CSRs: 10.9.2, 1.8.4

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

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

1.7.1	CMS has categorized sensitive Medicare data, FTI, and Privacy Act-protected data as sensitive information. These items are to be protected under the CMS Level 3 - High Sensitive security designation.	Sensitive Information Safeguard Requirements verify that the combinations of protection implemented for Level 3 sensitive data match those specified in the Business Partners Systems Security Manual, Section 4.1.1.3.	FISCAM TAC-1.1 IRS 1075 4.1@2 CMS Directed NIST 800-53 IA-5 NIST 800-53 RA-2 ARS RA-2.1 ARS RA-2.2 ARS RA-2.3 PISP 4.3.1.5 PISP 4.1.1.2

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

Related CSRs: 2.5.3, 2.7.1, 2.2.11, 10.6.2, 2.2.2, 2.2.10, 1.3.5

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

1.8 Minimum protection standards shall consider local factors.

	General Requirement Control Technique	Protocol	Reference
1.8.1	Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.	Review relevant policies and procedures for inclusion of the required security management features.	HIPAA 164.308(a)(1)(ii)(A) HIPAA 164.308(a)(1)(ii)(B) HIPAA 164.308(a)(1)(ii)(C) NIST 800-53 PS-8 ARS PS-8 HSPD-7 G(24) PISP 4.2.1.8

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

Related CSRs: 3.1.2, 1.9.2

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

	General Requirement Control Technique	Protocol	Reference
1.8.2	Local Information System risk factors are periodically assessed in accordance with the CMS Business RA Methodology, CMS IS RA Methodology, and NIST SP 800-30. The risk assessment is reviewed and updated annually or whenever significant modifications are made to a system, facility, or network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (policy, procedure, separating duties, security awareness and security training, testing/validating/editing, audit routines, audit trails/logs, alarms and fire extinguishing equipment, computer system automatic controls, manual controls, good housekeeping, secure disposal, authorizing/restricting access, relocating operations/equipment/records, modifying building/work environment, backup/encryption, insurance/bonding and maintenance/repair/replacement).	1. Review relevant policies and procedures for inclusion and directed use of the required process for determining the need for reassessment. 2. Review documentation verifying assessment of local risk factors in accordance with the reference. 3. Review relevant policies and procedures for inclusion and directed use of the required content. 4. Review the most recent risk assessment for documented inclusion of the required content.	CMS Directed ARS RA-3.CMS-1 FISCAM TSP-5.1.1 HIPAA 164.308(a)(1)(ii)(A) FISCAM TSP-1.1 NIST 800-53 CA-4 NIST 800-53 RA-3 NIST 800-53 RA-4 ARS CA-4.CMS-1 ARS RA-3.1 ARS RA-4.1 HSPD-7 G(24) ARS RA-4 PISP 4.1.4.4 PISP 4.1.1.3

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, 2.2.31, 3.5.2, 1.12.3, 5.9.9, 1.9.5

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

	General Requirement Control Technique	Protocol	Reference
1.8.3	Documentation is available to ensure that sensitivity level and criticality designations have been assigned for each system, and that these designations are commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.	Review documentation establishing that the required designations have been assigned with the considerations specified.	CMS Directed NIST 800-53 RA-2 ARS RA-2.1 PISP 4.1.1.2

Guidance: Review the BPSSM and apply sensitivity level and criticality designations in accordance with FIPS 199.

Related CSRs: 3.1.2

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

	General Requirement Control Technique	Protocol	Reference
1.8.4	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. Vulnerability scanning tools and techniques include the capability to readily update the list of vulnerabilities scanned at least quarterly or when significant new vulnerabilities are identified and reported.	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.	NIST 800-53 RA-5 ARS RA-5.1 ARS RA-5.0 ARS RA-5.2 PISP 4.1.1.5

Guidance: Review risk assessment.

Related CSRs: 1.6.6, 10.8.8

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

	General Requirement Control Technique	Protocol	Reference
1.8.5	The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	1. Review risk assessment policy for inclusion of the required factors. 2. Review the most recent high-level risk assessment for documentation of consideration of the required factors.	FISCAM TSP-1.1.2 HIPAA 164.308(a)(1)(ii)(A) NIST 800-53 RA-3 PISP 4.1.1.3

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

Related CSRs: 3.1.2, 2.7.1

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

	Control Technique	Protocol	Reference
1.8.6	Facilities housing sensitive and critical resources (i.e., key resources) have been identified and prioritized. All significant threat sources, both natural and manmade, to the physical well-being of sensitive and critical resources have been identified and related risks determined in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Adequate physical security controls have been implemented that are commensurate with the risks and magnitude of physical damage or access.	1. Review documentation supporting an assessment that all facilities housing sensitive and critical resources have been identified. 2. Review documentation supporting an assessment that all significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	FISCAM TAC-3.1.A.1 FISCAM TAC-3.1.A.2 NIST 800-53 PE-3 ARS PE-3.CMS-2 HSPD-7 D(8) HSPD-7 E(12) HSPD-7 F(19)(c) HSPD-7 H(25)(a) HSPD-7 J(27)(a) HSPD-7 J(27)(b) PISP 4.2.2.3

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

Related CSRs: 1.9.3

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

	Control Technique	Protocol	Reference
1.8.7	Top management initiates prompt actions to correct deficiencies and ensures that corrective actions are effectively implemented. Personnel are designated to assign, track, and update risk mitigation efforts. Designated personnel define and authorize corrective action plans, and monitor corrective action progress. Corrective actions are completed within 30 days for all vulnerabilities identified through risk assessment procedures.	1. Review documentation supporting consistent prompt action by top management to correct deficiencies. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSP-5.1.4 NIST 800-53 RA-3 ARS RA-3.CMS-2 PISP 4.1.1.3

Guidance: An approach is to have senior management approve the corrective action plan and have quarterly updates to the plan.

Related CSRs: 1.2.1, 1.12.3

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

	Control Technique	Protocol	Reference
1.8.8	Major systems and applications are approved by the managers whose missions they support. Final risk determinations and related management approvals, and written agreements with program officials on the security controls employed and residual risk are documented and maintained on file. (Such determinations and agreements may be incorporated in the system security plan.)	1. Confirm by inspection that the required documentation and agreements is on file. 2. Inspect documentation of approval for each major system and application by the specified manager. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSP-1.1.3 HIPAA 164.308(a)(1)(ii)(A) FISCAM TSP-5.1.3

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

Related CSRs: 3.1.2

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

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

	Control Technique	Protocol	Reference
1.9.1	Formal security and operational procedures and controls are implemented. Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records. System documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to facilitate analysis.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify by inspection that the system security plan contains the required controls. 3. Review documentation supporting the security and operational controls.	HIPAA 164.308(a)(1)(ii)(A) NIST 800-53 CM-2 NIST 800-53 SA-5 ARS CM-2.CMS-2 ARS SA-5.1 PISP 4.2.4.2 PISP 4.1.3.5

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

Related CSRs: 1.11.2, 1.4.3, 9.8.4, 9.8.5, 10.4.1

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

	General Requirement Control Technique	Protocol	Reference
1.9.2	A system security plan has been prepared and approved, in accordance with the CMS SSP Methodology, to cover every application and system categorized as a Major Application (MA) or General Support System (GSS).	1. Review documentation establishing that preparation of the plan was in accordance with the CMS SSP Methodology. 2. Review documentation verifying coverage by system security plans for all applications categorized as MA and GSS. 3. Review SSP to determine if approval signatures are included	CMS Directed NIST 800-53 CA-2 NIST 800-53 CA-3 NIST 800-53 PL-2 NIST 800-53 RA-2 NIST 800-53 SA-5 ARS CA-2.3 ARS CA-3.CMS-1 ARS PL-2.CMS-1 ARS RA-2.1 ARS SA-5.CMS-2 NIST 800-53 CM-2 PISP 4.1.4.2 PISP 4.1.4.3 PISP 4.2.4.2 PISP 4.1.2.2 PISP 4.1.1.2 PISP 4.1.3.5 ARS SC-CMS-6.CMS-1 PISP 4.3.4
	Guidance: Refer to the CMS System Security Plans Methodology for further guidance.		Related CSRs: 9.4.1, 3.2.3, 3.3.2, 3.4.5, 3.5.2, 3.5.3, 3.5.5, 3.6.2, 3.6.3, 1.8.1, 1.5.4, 1.12.4
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***
1.9.3	A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties, and (3) covers the topics prescribed by OMB Circular A-130 such as: (a) system/application rules; (b) security awareness and security training; (c) promotes a continuing awareness of information security issues and threats; (d) personnel controls/personnel security; (e) incident response capability; (f) continuity of support/contingency planning; (g) technical security/technical controls; (h) system interconnection/information sharing; and (i) public access controls.	1. Review documentation verifying that a security plan covers all major facilities and operations. 2. Review documentation verifying that the security plan has been approved by all key affected parties. 3. Inspect the security plan to confirm that it covers all of the specified topics.	FISCAM TSP-2.1 HIPAA 164.310(a)(1) HIPAA 164.310(a)(2)(ii) HIPAA 164.310(a)(2)(i) HIPAA 164.308(a)(4)(i) NIST 800-53 AT-2 NIST 800-53 CA-3 NIST 800-53 SA-5 ARS AT-2.CMS-1 ARS SA-5.CMS-1 HSPD-7 H(25)(b) PISP 4.2.9.2 PISP 4.1.3.5 ARS CA-3.CMS-1 PISP 4.1.4.3
	Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 6.3.13, 10.7.2, 2.10.5, 1.6.3, 1.8.6, 6.1.1, 1.1.7, 1.6.1, 1.6.2, 1.6.4
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***
1.9.4	The following are accomplished and documented: (1) current system configuration documentation, including links to other systems; (2) security configuration documentation; (3) hardware/software installation and maintenance, including patch management, review and testing for security features; (4) inventory records; (5) security testing; and (6) checking for malicious software.	1. Review the security plan for inclusion of the required elements. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation supporting completion of the required security testing. 4. Review system configuration documentation for inclusion of links to other systems.	HIPAA 164.308(a)(5)(ii)(B) HIPAA 164.310(a)(2)(iv) NIST 800-53 CM-2 NIST 800-53 MA-2 NIST 800-53 SA-5 ARS MA-2.1 ARS SA-5.CMS-4 PISP 4.2.4.2 PISP 4.2.5.2 PISP 4.1.3.5
	Guidance: Policies and procedures should exist that address these control objectives.		Related CSRs: 5.9.4, 5.12.1, 2.5.1, 6.3.16, 5.9.9, 5.12.2, 6.3.15, 10.7.3, 10.7.4, 10.9.1
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***

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

General Requirement Control Technique		Protocol	Reference
1.9.5	The system security plan is reviewed and updated to reflect current conditions at least annually, or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting conduct of the required periodic reviews. 3. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.	FISCAM TSP-2.2 NIST 800-53 PL-3 ARS PL-3 PISP 4.1.2.3

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

Related CSRs: 1.8.2, 1.12.6

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

1.9.6	The system security plan documents a security management structure with adequate independence, authority and expertise.	1. Verify by inspection that the system security plan contains the required management structure. 2. Review documentation supporting the assertion that the security management structure meets the stated requirements.	FISCAM TSP-3.1.1

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

Related CSRs: 1.5.3

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

1.9.7	Information system continuous monitoring activities include: (1) configuration management; (2) control of information system components; (3) security impact analyses of changes to the system; (4) on-going assessment of security controls; and (5) status reporting.	1. Examine the security control monitoring procedures to determine if the required controls are included. 2. Examine policies and procedures to determine if specific parties are assigned the stated responsibilities. 3. Examine policies and procedures to determine if the specified actions are defined. 4. Interview selected personnel with security control monitoring responsibilities.	NIST 800-53 CA-7 ARS CA-7.CMS-1 PISP 4.1.4.7

Guidance: Security monitoring measures should be consistent with NIST SP 800-37.

Related CSRs: 10.2.9, 10.7.6

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

1.9.8	A management-initiated independent review or audit of the security controls of all Medicare systems, including interconnected systems, and applications processing sensitive information is performed at least every three years and when a significant change has occurred.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying conduct of an independent review or audit at least every three years and when a significant change has occurred. 3. Review documentation verifying independent review includes interconnect system security controls.	IRS 1075 6.3@9.1 FISCAM TSP-5.1.2 NIST 800-53 AC-5 ARS AC-5.CMS-5 PISP 4.3.2.5

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: 1.12.1

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

	General Requirement Control Technique	Protocol	Reference
1.9.9	The CMS Business Partner System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self-assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, CMS, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10) authorization lists that include the designation of the individual responsible for handling security violations and each individual (or position title) responsible for individual assets; and (11) lists of other security records such as audit trails/logs and visitor sign-in sheets. Include all other CMS directed or Business Partners System Security Manual directed documents.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.	HIPAA 164.316(b)(1) HIPAA 164.316(b)(2)(ii) HIPAA 164.316(b)(2)(iii) CMS Directed NIST 800-53 SA-5 ARS SA-5.CMS-3 HSPD-7 D(8) PISP 4.1.3.5

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

Related CSRs: 2.2.32, 2.2.31, 3.3.2, 1.12.7

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

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

1.10.1	For prospective employees, references are contacted and background checks performed prior to granting access to CMS sensitive data or systems. Any conditions that allow access prior to completion of the screening process, including the compensating controls that are place, must be documented.	1. Inspect personnel records to confirm that references have been contacted and background checks have been performed. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documented conditions that allow access prior to completion of the screening process, as well as the in-place controls that compensate for allowing this type of access.	FISCAM TSP-4.1.1 CMS Directed NIST 800-53 PS-3 ARS PS-3.0 PISP 4.2.1.3

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

Related CSRs: 1.1.6, 1.1.2

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

1.10.2	Regular scheduled vacations exceeding several days and job or shift rotations are required for those personnel using sensitive information.	1. Inspect a sample of personnel records to confirm compliance with the required vacation policy. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review staff assignment records to confirm that job and shift rotations occur.	FISCAM TSP-4.1.5 FISCAM TSD-1.1.7 FISCAM TSP-4.1.4

Guidance: An approach is a policy developed that requires employees using sensitive information to take a minimum of 24 hrs continuous vacation. Personnel whose duties or position gives them access to input or modify sensitive data in such a manner that fraud may be committed should be periodically rotated into different jobs or different shift rotations to introduce other personnel into the process. These rotations increase the likelihood that collaborative fraudulent activities by multiple employees will be disrupted and identified.

Related CSRs: 1.4.1, 2.5.2

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

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

	General Requirement Control Technique	Protocol	Reference
1.10.3	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 UserIDs and passwords; (4) ensuring access to official files created by terminated employees; (5) immediately escorting involuntarily terminated employees out of the entity's facilities; and (6) identifying the period during which nondisclosure requirements remain in effect.	1. Review termination and transfer procedures for inclusion of the required processes. 2. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist. 3. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.	FISCAM TSP-4.1.6 HIPAA 164.308(a)(3)(ii)(C) NIST 800-53 AC-2 NIST 800-53 IA-4 NIST 800-53 PS-4 NIST 800-53 PS-5 ARS AC-2.CMS-5 ARS PS-4.0 ARS PS-5 PISP 4.3.2.2 PISP 4.2.1.4 PISP 4.2.1.5
	Guidance: These items need to be addressed as part of a HR Termination/Transfer procedure.	Related CSRs: 2.9.17, 2.2.18, 2.9.18	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	☑ ***COB***
1.10.4	Security is notified immediately when system users are terminated or transferred.	1. Review relevant policies and procedures for inclusion and directed use of the required procedure. 2. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.	FISCAM TAC-2.1.6
	Guidance: Users who continue to have access to critical or sensitive resources pose a major threat, especially those who may have left under acrimonious circumstances.	Related CSRs: 2.2.18, 2.9.17	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	☑ ***COB***
1.10.5	Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.	1. Review documentation establishing that reinvestigation policies for each position are consistent with the specified criteria. 2. Inspect personnel records to confirm sensitive position have had background reinvestigations performed within the required period.	FISCAM TSP-4.1.2 NIST 800-53 PS-3 ARS PS-3.0 PISP 4.2.1.3
	Guidance: CMS will provide future direction.	Related CSRs: 2.5.2	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	☑ ***COB***
1.10.6	Confidentiality or security agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) are required for CMS Business Partner Medicare employees and their contractors assigned to work with sensitive information before access is authorized.	1. Review policies on confidentiality or security agreements. 2. Determine whether confidentiality or security agreements are on file. 3. Review a sampling of agreements.	FISCAM TSP-4.1.3 HIPAA 164.314(a)(1) HIPAA 164.308(b)(1) HIPAA 164.308(b)(4) NIST 800-53 AC-2 NIST 800-53 PL-4 NIST 800-53 PS-6 NIST 800-53 PS-7 ARS AC-2.CMS-4 ARS PL-4.CMS-1 ARS PL-4.CMS-2 ARS PS-6 ARS PS-7.CMS-1 PISP 4.3.2.2 PISP 4.1.2.4 PISP 4.2.1.6 PISP 4.2.1.7
	Guidance: One method would be to include the agreements as part of the procedural policy and include a standard contract clause for all procurements.	Related CSRs: 1.11.1	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF***	☑ ***COB***

	General Requirement Control Technique	Protocol	Reference
1.11	Disclosure of sensitive information by CMS Business Partners to their subcontractors shall be controlled.		
1.11.1	Disclosure of sensitive information is prohibited unless specifically authorized by statute.	1. Review Authorized Disclosure Agreements. 2. Review relevant policies for inclusion and directed use of the required directive.	IRS 1075 11.1@1.1 CMS Directed IRS 1075 11.1@1.3 IRS 1075 11.1@1.4 IRS 1075 11.1@1.2 HIPAA 164.306(a)(3)
Guidance:	Examples of statutes that should be reviewed include, but are not limited to, state and federal statutes involving disclosure mandates or restrictions including the HIPAA Privacy Rule, and statutes covering special circumstances.	Related CSRs: 1.10.6, 1.4.2, 1.3.6	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.11.2	Written contracts or other arrangements require the inclusion of the CMS Core Security Requirements to protect the integrity, confidentiality, and availability of the electronically exchanged data. Contractor compliance with CMS information security requirements is monitored to ensure adequate security. The contractor selection process assesses the contractor's ability to adhere to and support CMS' information security policies and standards. The CMS Business Partner maintains a list of all contracts or other arrangements with other organizations (include organization name and location, contract or agreement number, and purpose). The list of contracts is provided to CMS in an MS Word document with the annual CAST submission.	1. Review documented arrangements/contracts for security content. 2. Verify risk-based decision is justified.	CMS Directed NIST 800-53 AC-2 NIST 800-53 AC-6 NIST 800-53 PS-7 NIST 800-53 SA-4 NIST 800-53 SA-9 ARS AC-2.CMS-4 ARS AC-6.CMS-3 ARS PS-7.CMS-1 ARS SA-4.CMS-1 PISP 4.3.2.2 PISP 4.3.2.6 PISP 4.2.1.7 PISP 4.1.3.4 PISP 4.1.3.9
Guidance:	A contract between a Business Partner and another organization in which the other organization agrees to electronically exchange data and protect the integrity and confidentiality of the data exchanged should be completed prior to the exchange of any data.	Related CSRs: 1.5.7, 1.9.1	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.11.3	The CMS Business Partner has obtained satisfactory assurances that all external business associates provide appropriate safeguards for CMS sensitive information. Before issuing external business associates (i.e., contractors, subcontractors) UserIDs to gain access to CMS sensitive systems, written approval is received from the Business Partner CIO or his/her designated representative.	1. Review the implemented safeguards. 2. Ensure satisfactory assurances have been provided.	HIPAA 164.308(b)(1) HIPAA 164.314(a)(1) NIST 800-53 AC-6 ARS AC-6.CMS-3 NIST 800-53 IA-4 ARS IA-4.CMS-2 PISP 4.3.2.6 PISP 4.3.1.4
Guidance:	A good approach may be to provide a risk-based solution. All contracts should be part of the security profile and available to the SSO for review.	Related CSRs: 2.14.2	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.11.4	Management has authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor), and controls have been established and disseminated to the owners of the interconnected systems. A signed Interconnection Security Agreement (ISA) is recorded for each system interconnection, and remote locations follow all CMS information security policies. System interconnections are monitored and controlled on an on-going basis. In addition, system interconnections are recorded in the Information Security (IS) Risk Assessment (RA).	1. Review relevant policies and procedures for inclusion of the required process. 2. Review interconnected system agreements and established controls.	NIST 800-53 CA-3 ARS SC-CMS-6.CMS-1 PISP 4.1.4.3 PISP 4.3.4 ARS CA-3.CMS-1
Guidance:	Appropriate organizational officials should approve information system interconnection agreements. NIST SP 800-47 provides guidance on interconnecting information systems.	Related CSRs: 2.14.2	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

	General Requirement Control Technique	Protocol	Reference
1.11.5	Service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. Third-party providers of information system services are monitored to ensure that they employ adequate security controls in accordance with established service level agreements, and applicable federal laws, directives, policies, regulations, standards, and guidance.	1. Review service level agreements and established controls. 2. Review relevant policies and procedures for inclusion of the required process.	NIST 800-53 SA-9 ARS SA-9.0 PISP 4.1.3.9
Guidance:	Appropriate organizational officials should approve service level agreements.	Related CSRs:	5.7.5, 5.10.1, 5.10.4, 5.9.1, 5.9.2
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.12	Descriptions of Medicare operations, records, and assets are validated once a year.		
1.12.1	To provide reasonable assurance that sensitive information is adequately safeguarded, an annual self-assessment and compliance review is conducted which addresses the safeguard requirements imposed by CMS. A copy of the self-assessment is submitted to CMS.	1. Review audit data confirming execution of the review process at least once a year. 2. Review relevant policies and procedures for inclusion of the required process. 3. Review documentation confirming submittal of the most recent self assessment to CMS.	HIPAA 164.316(b)(2)(iii) IRS 1075 6.3@1.1 HIPAA 164.308(a)(8) IRS 1075 6.3@1.3 IRS 1075 6.3@1.2 IRS 1075 6.3@1.4 NIST 800-53 CA-2 ARS CA-2 CMS Directed OMB A-123 (Revised) PISP 4.1.4.2
Guidance:	Ensure that a CISS self-assessment is completed once a year and that if a management-initiated compliance audit or review is required, it is completed once a year and independently verified.	Related CSRs:	2.5.8, 1.9.8
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.12.2	The System Owner/Manager, System Maintainer, or Senior Management designee signs the SSP and certification package. By doing so, they acknowledge the risk to systems under their control and determine the acceptable level of risk.	Inspect the SSP and certification package for the required signatures.	CMS Directed
Guidance:	Review SSP certification package.	Related CSRs:	2.7.1
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
1.12.3	The safeguard selection decisions and the risk assessment reports are carefully analyzed to determine whether the security requirements in place adequately mitigate vulnerabilities. The CMS Business Partner is responsible for approving any necessary corrective action plans.	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. 4. Examine documentation supporting completion of the required review.	CMS Directed NIST 800-53 RA-3 PISP 4.1.1.3
Guidance:	Review risk assessment and safeguard selection for mitigation of risks and provide recommendations. An approach is to provide annual sign-off, by senior management, on the Corrective Action Plan.	Related CSRs:	1.8.2, 1.8.7, 1.2.1
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

1.12.4 The CMS Business Partner's systems security certification is completed annually and is fully documented. Whenever new security controls are added, the security controls are tested and the system recertified.

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

CMS Directed
NIST 800-53 AC-5
ARS AC-5.CMS-5
PISP 4.3.2.5

Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM. Related CSRs: 1.9.2

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

1.12.5 A certification assessment of the security controls in the information system is conducted to validate that the controls are implemented correctly, operate as expected, and provide adequate protection in compliance with the security requirements for the information system.

1. Review documentation confirming that the last CMS Business Partner's systems security certification or recertification was completed within the last year or whenever new security controls are added.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

NIST 800-53 CA-4
PISP 4.1.4.4

Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM. Related CSRs: 6.3.2, 10.7.6

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

1.12.6 CMS Business Partner office facilities processing sensitive information are subjected to an annual self-assessment.

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

CMS Directed
IRS 1075 6.3@9.2
FISCAM TSP-5.1.1

Guidance: Annual self-assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan. Related CSRs: 2.12.1, 1.9.5

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

1.12.7 Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.

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

HIPAA 164.316(b)(2)(i)
IRS 1075 6.3@11.1
CMS Directed

Guidance: Inspection, self-assessment, and corrective action reports are an important means of identifying areas of noncompliance and remedial actions performed to correct noncompliance. Related CSRs: 1.9.9

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

1.13 General workstation security requirements shall be established.

1.13.1 The following workstation security requirements are specified and implemented: (1) what workstation functions can be performed, (2) the manner in which those functions are to be performed, (3) and the physical attributes of the surroundings of a specific workstation or class of workstation that can access CMS sensitive information.

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

HIPAA 164.310(b)
NIST 800-53 PE-5
ARS PE-5.0
PISP 4.2.2.5

Guidance: One approach would be to address all the local workstations as well as the workstations used at home. Related CSRs: 7.3.5, 7.3.1, 7.4.1, 7.5.1, 10.6.3, 10.8.4

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

	General Requirement Control Technique	Protocol	Reference
1.13.2	Controls prohibit employees from bringing their personally owned computer equipment and software into the workplace. Employees are prohibited from using personally-owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information, unless the use of such personally-owned systems has been approved.	1. Review the specified policy. 2. Review the controls that prohibit this.	CMS Directed NIST 800-53 AC-20 PISP 4.3.2.20
	Guidance: Bringing personal computers into the workplace creates vulnerabilities to Medicare resources and could compromise sensitive data.		Related CSRs: 2.2.23, 6.2.1
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.3	All CMS-owned software (such as CAST) is secured at close of business or anytime that it is not in use. Manuals and diskettes or CD-ROMs are stored out of sight in desks or file cabinets.	1. Interview programmers and system manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming enforcement of the required process.	CMS Directed
	Guidance: Policies and procedures should exist that address these control objectives.		Related CSRs: 10.7.1
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.4	If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the process used to assure compliance with the required policy.	CMS Directed NIST 800-53 AC-20 ARS AC-20.CMS-1 PISP 4.3.2.20
	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: 2.2.28
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.5	Measures are established for controlling the use of laptops, notebooks, and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.	Determine the effectiveness of controlling portable devices by review business partner mobile computing policies.	CMS Directed
	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: 2.2.28
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.6	Users are prohibited from installing desktop modems.	1. Examine user's desktops for compliance. 2. War-Dialing. 3. Review the policy on addressing desktop modems.	ARS SC-CMS-1.CMS-1 PISP 4.3.4
	Guidance: If no policy currently exists, one should be created. If no process for testing exists, one should be developed.		Related CSRs: 10.8.1
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
1.13.7	The connection of portable computing or portable network devices on the CMS claims processing network is restricted to approved devices only. Removable hard drives and/or a FIPS-approved method of cryptography are employed to protect information residing on portable and mobile information systems.	Review documentation restricting the use of portable devices.	NIST 800-53 AC-19 ARS AC-19.1 ARS PE-CMS-2.CMS-1 ARS PE-CMS-3.CMS-1 ARS AC-19.3 PISP 4.3.2.19 PISP 4.2.2.4 PISP 4.2.2.3
	Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.		Related CSRs: 1.5.6, 2.5.5
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

	General Requirement Control Technique	Protocol	Reference
1.13.8	If usage is approved, the users of personally-owned information systems must adhere to enterprise-wide strict terms and conditions that address the following: (1) types of applications that can be accessed from personally-owned information systems; (2) maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (3) prevention of access to federal information on personally-owned information system by other users of the system; (4) use of VPN and firewall technologies; (5) use of and protection against the vulnerabilities of wireless technologies; (6) maintenance of adequate physical security controls; (7) use of virus and spyware protection software; and (8) installation of and upgrading security capabilities for installed software (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions).	1. Review documentation restricting the use of personally-owned devices. 2. Review existing policies and procedures to ensure prohibition of personally-owned system.	NIST 800-53 AC-20 ARS AC-20.0 PISP 4.3.2.20
	Guidance: Establish a process to review all personally-owned systems before they are connected to the claims processing network.	Related CSRs: 6.2.1, 2.2.24, 5.12.1, 10.2.2, 2.2.9, 10.10.5	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc***	☑ ***DC*** ☑ ***CWF***	☑ ***COB***
1.13.9	Before connecting portable or mobile information systems to Medicare claims processing networks, the following is performed: (1) update virus protection software; (2) scan for malicious code using approved methods; (3) scan the information system for critical software updates and patches; (4) conduct primary operating system integrity checks; and (5) disable unnecessary hardware (e.g., wireless).	Review documentation restricting the use of portable and mobile devices.	NIST 800-53 AC-19 PISP 4.3.2.19
	Guidance: Establish a process to review all portable and mobile systems before they are connected to the claims processing network.	Related CSRs: 2.2.24, 5.12.1, 10.2.2, 5.12.2	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc***	☑ ***DC*** ☑ ***CWF***	☑ ***COB***
1.13.10	An automated method is used on demand, and at least weekly, to examine a sample of network systems to determine if unnecessary network services are available. A complete review is performed on demand, and at least monthly.	1. Review existing policies and procedures to ensure prohibition of modems specified. 2. Review existing procedures to ensure sampling requirement defined sufficiently to ensure adequate coverage of all assets.	NIST 800-53 CM-7 ARS SC-CMS-2.CMS-1 ARS CM-7.1 PISP 4.2.4.7 PISP 4.3.4
	Guidance: Establish an automated process to examine and review a sample of all connected systems.	Related CSRs: 10.8.7	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc***	☑ ***DC*** ☑ ***CWF***	☑ ***COB***

2. *Access Control*

2.1 Audit trails/logs shall be maintained.

	General Requirement Control Technique	Protocol	Reference
2.1.1	The content of audit records generated by individual components throughout the system is managed centrally. User account activity audits are conducted using automated audit controls. Auditing of administrator activities is enabled and verified.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the automated controls installed to implement the required process. 3. Inspect activity audit logs to confirm continuing use of the required process.	HIPAA 164.312(b) NIST 800-53 AC-2 NIST 800-53 AC-13 NIST 800-53 AU-2 NIST 800-53 AU-3 ARS AC-2.4 ARS AC-13.1 ARS AU-3.2 PISP 4.3.2.2 PISP 4.3.2.13 PISP 4.3.3.2 PISP 4.3.3.3
	Guidance: Automated tools support real-time and after-the-fact monitoring. They assist in identifying questionable data access activities, investigating breaches, responding to potential weaknesses, and assessing the security program. Audit reduction tools and/or "intelligent" methods of correlating log data may be used to detect unauthorized activity and reduce volumes to manageable size.	Related CSRs: 9.1.1, 9.1.2, 9.3.1, 9.5.1, 9.6.7, 4.2.2, 3.1.5, 9.3.3	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc***	☑ ***DC*** ☑ ***CWF***	☑ ***COB***

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.1.2	Computer systems processing sensitive information are secured from unauthorized access. All security features are available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing sensitive information is accountable.	1. Review documentation identifying all security features of each hardware and software item in the system, and the extent to which each feature is available and activated. 2. Review documentation establishing that the computer systems processing sensitive information are secured from unauthorized access. 3. For a sample of hardware and software security features, obtain demonstrations of feature operation. 4. Review documentation describing how audit facilities are utilized to assure that everyone accessing a computer system containing sensitive information is accountable.	HIPAA 164.310(c) IRS 1075 5.6@4.1 IRS 1075 5.6@3.3 NIST 800-53 AU-2 PISP 4.3.3.2

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, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 2.2.3, 2.5.1, 2.2.21, 9.3.3

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

2.1.3	Proper logging of administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations is enabled.	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 activities are being logged.	NIST 800-53 AC-13 ARS AC-13.CMS-2 PISP 4.3.2.13

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

Related CSRs: 2.9.16, 2.9.15

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

2.1.4	Privilege restrictions deny non-administrator access to administrator tools, scripts, and utilities. All file system access not explicitly required for system, application, and administrator functionality is disabled.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review system privilege restrictions to administrator functions.	NIST 800-53 AC-6 ARS AC-6.CMS-1 ARS AC-6.CMS-2 PISP 4.3.2.6

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

Related CSRs: 2.9.15, 2.9.16, 3.2.3, 10.7.8, 2.11.2

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

	General Requirement Control Technique	Protocol	Reference
2.1.5	All activity involving access to and modifications of sensitive or critical files is logged.	1. Validate the types of files involved and the features are turned on or coding has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation describing how compliance with this requirement is assured. This should include documentation specifically designating all files considered sensitive or critical, with identification of the corresponding logging methodology for each of these files. 4. Inspect samples of the specified audit logs to confirm continuing use of the required process.	FISCAM TAC-4.1

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, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 9.3.3

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

	General Requirement Control Technique	Protocol	Reference
2.1.6	Access to audit trails/logs is restricted. Audit information and audit tools are protected from unauthorized access, modification, and deletion. Audit functions are not performed by security personnel responsible for administering access control. Automated mechanisms are employed and restricted to hardware-enforced, “write-once” media (e.g., CD-R, not CD-RW) for recording audit information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required restrictions. 3. Review security software settings and compare with system security policies and procedures. 4. Inspect a sample of audit log access lists.	CMS Directed NIST 800-53 AC-5 NIST 800-53 AU-9 ARS AC-5.CMS-1 ARS AU-9.1 PISP 4.3.2.5 PISP 4.3.3.9

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, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 9.3.3

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

	General Requirement Control Technique	Protocol	Reference
2.1.7	The audit trail includes sufficient information to establish what events occurred and who or what caused them. The audit trail information includes: (1) date and time of the event logged; (2) component of the information system where the event occurred; (3) type of event; subject identify; and (4) outcome (success or failure) of the event. A capability is provided to compile audit records from multiple components throughout the system into a system-wide (logical or physical) time correlated audit trail. Additionally, a capability is provided to manage the selection of events to be audited by individual components of the information system.	1. Review a sample of event logs and audit records to confirm the required content. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed NIST 800-53 AU-2 NIST 800-53 AU-3 NIST 800-53 AU-11 ARS AU-2.1 ARS AU-2.2 ARS AU-3.1 PISP 4.3.3.2 PISP 4.3.3.3

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, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 9.3.3

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

	General Requirement Control Technique	Protocol	Reference
2.1.8	Audit records are generated for the following events: (1) user account management activities; (2) failed and successful log-ons; (3) security policy modifications; (4) use of administrator privileges; (5) system shutdown; (6) system reboot; (7) system errors; (8) application shutdown; application restart; (9) application errors; (10) file creation; (11) file deletion; (12) file modification; and (13) file access.	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 activities are being logged.	NIST 800-53 AU-2 ARS AU-2.0 PISP 4.3.3.2

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

Related CSRs: 10.2.9

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

2.1.9	Disclosures and modifications of personal information, including protected health and financial information are recorded. The log includes: information type, date, time, receiving party, and releasing party. A capability is provided to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. The content of audit records generated by individual components throughout the system is managed centrally.	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 activities are being logged.	NIST 800-53 AU-3 ARS AU-3.2 ARS AU-3.1 ARS AU-3.CMS-1 HIPAA 164.528(b)(2) PISP 4.3.3.3

Guidance: Maintain, and periodically review, audit logs for critical application systems, system events, and information disclosures. Audit logs may become evidence in legal proceedings, so care should be taken to protect their integrity

Related CSRs: 1.4.2, 10.6.2

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

2.1.10	All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.	1. Inspect device configurations to confirm that all detected errors that can be logged are being logged. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Determine that audit logs have sufficient detail to assist with fault isolation and resolution of security abnormalities.	CMS Directed NIST 800-53 SI-11 ARS SI-11.0 PISP 4.2.6.11

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

Related CSRs: 4.1.1

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

2.1.11	Output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system is retained in accordance with federal law and all applicable NARA requirements. However, they are retained minimally for 90 days, old logs are archived, and log archives retained for one (1) year.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that audit logs are being retained for the same period as the related claim. 3. Inspect a sample of audit data confirming that the required reviews have been conducted.	CMS Directed HIPAA 164.308(a)(1)(ii)(D) NIST 800-53 AU-11 NIST 800-53 SI-12 ARS AU-11.0 ARS SI-12.1 PISP 4.3.3.11 PISP 4.2.6.12

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, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 9.3.3, 10.3.6

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

	General Requirement Control Technique	Protocol	Reference
2.1.12	Automated utilities are used to review audit logs daily for unusual, unexpected, or suspicious behavior. Manual reviews are performed randomly on demand, but at least once every 30 days. Administrator groups are inspected on demand but at least once every 7 days to ensure unauthorized administrator accounts have not been created.	1. Review audit review procedures. 2. Review audit logs. 3. Validate the system is operationally enabled.	NIST 800-53 AC-2 NIST 800-53 AC-13 NIST 800-53 AU-6 ARS AC-2.0 ARS AC-13.CMS-3 ARS AU-6.CMS-6 ARS AU-6.CMS-5 ARS AU-6.CMS-4 PISP 4.3.2.2 PISP 4.3.2.13 PISP 4.3.3.6

Guidance: Procedures should exist which describe how to respond to an alert generated by the automated log review utilities.

Related CSRs: 10.2.9, 10.3.6

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

2.1.13	The information system provides an audit reduction and report generation capability. Audit records are processed automatically for events of interest based upon selected, event criteria. Time stamps generated by internal system clocks that are synchronized system-wide are used in audit record generation.	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 audit reduction and report generation is being performed. 3. Inspect a sample of system times to ensure all system clocks are synchronized.	NIST 800-53 AU-7 NIST 800-53 AU-8 ARS AU-7 ARS AU-8 PISP 4.3.3.7 PISP 4.3.3.8

Guidance: Maintain, and periodically review, audit logs for critical application systems and system events. Since audit logs may become too large to review, audit reduction tools should be used to capture important and critical audit events. Audit logs may become evidence in legal proceedings, so care should be taken to protect their integrity

Related CSRs: 3.1.5

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

2.1.14	Sufficient audit record storage capacity is allocated and auditing is configured to provide a warning when allocated capacity reaches ninety percent (90%). In the event of an audit failure or the audit storage capacity being reached, the information system alerts appropriate officials and takes the additional actions as established by policy (e.g., shutdown the information system, stop generating audit records, overwrite the oldest audit records in the case that storage media is unavailable).	1. Inspect the audit log configuration to confirm that the system alerts the appropriate officials in the event of an audit failure or the audit storage capacity being reached. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation describing implementation of the required restriction. 4. Inspect the audit log configuration to confirm that the audit log storage capacity has set in accordance to the policy.	NIST 800-53 AU-5 ARS AU-5.0 CMS Directed NIST 800-53 AU-4 ARS AU-4 ARS AU-5.1 PISP 4.3.3.4 PISP 4.3.3.5

Guidance: Establish an audit record storage capacity limit and configure the system to prevent exceeding the established limit. The system should be configured to provide a warning and alert appropriate officials when the allocated audit record storage volume reaches 90% of maximum audit record storage capacity. Policy should establish what additional actions should be taken if there is an audit failure or when the audit storage capacity is reached.

Related CSRs: 10.2.9

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

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

2.2.1 Procedures are implemented for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges). Management regularly reviews the list of persons with physical access to sensitive facilities. This review is conducted at least once every 30 days.

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.
3. Inspect a sample of audit data confirming that the required process is consistently used.

HIPAA 164.312(d)
FISCAM TAC-3.1.A.4
ARS PE-2.0
HIPAA 164.308(a)(3)(i)
HIPAA 164.310(a)(1)
HIPAA 164.310(a)(2)(iii)
NIST 800-53 PE-2
PISP 4.2.2.2

Guidance: Policies and procedures for limiting physical access ensure that properly authorized access is allowed. Access to sensitive facilities should be limited to personnel with a legitimate need for access to perform their duties.

Related CSRs: 2.4.2, 2.8.2, 10.1.2, 2.8.6

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

2.2.2 Management analyzes local circumstances to determine space, container, and other security needs at individual facilities that meet or exceed the minimum protection requirements for the CMS Level 3 - High Sensitivity security designation.

Review documentation establishing that a location-specific Risk Analysis was conducted in development of each applicable System Security Plan.

CMS Directed
IRS 1075 4.2

Guidance: See the Business Partners Security Manual for additional information and guidance.

Related CSRs: 1.7.1

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

2.2.3 Access to facilities/data centers is limited to those individuals who routinely need access through the use of guards, identification badges, or physical authentication devices, such as biometrics and/or smart card/PIN combination.

1. Review documentation designating specific individuals who are allowed access, and identifying the associated access control method used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review a sample of audit data confirming consistent use of the required access process.

FISCAM TAC-3.1.A.3
NIST 800-53 PE-3
ARS PE-3.1CMS-1
PISP 4.2.2.3

Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties.

Related CSRs: 1.3.13, 2.1.2, 2.5.5, 9.2.1, 2.9.4, 2.9.3

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

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

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

IRS 1075 4.3@24
FISCAM TAC-3.1.A.2
NIST 800-53 PE-6
ARS PE-6.1
ARS PE-6.2
PISP 4.2.2.6

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

Related CSRs: 3.6.5

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

	General Requirement Control Technique	Protocol	Reference
2.2.5	Signs denoting restricted areas are prominently posted and separated from non-restricted areas by physical barriers that control access. All entrances have controlled access (e.g., electronic access control, key access, door monitor) and the main entrance to restricted areas is manned. Physical accesses are monitored through audit trails and apparent security violations investigated and remedial action taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required controls. 3. Review a sample of audit data confirming consistent use of the required access process. 4. Inspect physical access audit trails to confirm that the physical accesses are being monitored.	IRS 1075 4.3@3.1 CMS Directed IRS 1075 4.3@3.2 IRS 1075 4.3@3.3

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: 2.8.3, 5.2.6

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

2.2.6	Secured areas/perimeters designed to prevent undetected entry by unauthorized persons during non-working hours are: (1) enclosed by slab-to-slab walls, constructed of approved materials, and supplemented by periodic inspection or other approved protection methods; (2) Any lesser-type partition is supplemented by UL-approved electronic intrusion detection and fire detection systems; (3) Unless intrusion detection devices are used, all doors entering the space are locked and strict key or combination control is exercised. In the case of a fence and gate, the fence has intrusion detection devices or is continually guarded and the gate is either guarded or locked with intrusion alarms; and (4) The space is cleaned during working hours in the presence of a regularly assigned employee.	1. Review documentation confirming that secured area/perimeters have the required features. 2. Inspect a sample of audit data confirming that the space is cleaned during working hours in the presence of a regularly assigned employee. 3. Inspect a sample of audit data confirming that the secured area/perimeters are consistently secured at the end of working hours, and found secured when opened for business. 4. Confirm by inspection that the required electronic intrusion devices are in use.	IRS 1075 4.3@13.1 CMS Directed NIST 800-53 PE-3 ARS PE-3.CMS-2 PISP 4.2.2.3

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: 7.3.2

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.2.7	Security rooms, if used, include the following features: (1) entire room is enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection; (2) all doors entering the space are locked with approved locking systems; (3) any glass in doors or walls is security glass (a minimum of two layers of 1/8-inch plate glass with .060-inch [1/32] vinyl interlayer, nominal thickness is 5/16-inch); (4) plastic glazing material is not acceptable; (5) vents and/or louvers are protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station, and is given top priority for guard/police response during any alarm situation; and (6) cleaning and maintenance is performed in the presence of an employee authorized to enter the room.	If Security Rooms are used, review documentation confirming that each includes all of the required features.	IRS 1075 4.3@10 IRS 1075 4.3@11 CMS Directed IRS 1075 4.3@9.2 IRS 1075 4.3@9.1 IRS 1075 4.3@9.4 IRS 1075 4.3@9.3
	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:	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***
2.2.8	Locking Systems for Secured Areas and Security Rooms - High-security pin-tumbler cylinder locks are used that meet the following requirements: (1) key-oriented mortised or rim-mounted deadlock bolt; (2) dead bolt throw of one inch or longer; (3) double-cylinder design; (4) cylinders have five or more pin tumblers; (5) if bolt is visible when locked, it contains hardened inserts or is made of steel; and (6) both the key and the lock are "Off Master." Convenience-type locking devices (e.g., card keys, sequence button-activated locks, etc.) used in conjunction with electric strikes are authorized for use during working hours only. Keys to secured areas are never in personal custody of an unauthorized employee and combinations are stored in a security container.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.	IRS 1075 4.3@22 IRS 1075 4.3@23.1 IRS 1075 4.3@23.3 CMS Directed
	Guidance: Security rooms are constructed to resist forced entry and their primary purpose is to store protectable material. Secured areas are interior areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours. The minimum requirements for their locking systems, as stated in this requirement, is contained in BPSSM Section 4. (Also refer to BPSSM Section 4 for additional information on security rooms and secured areas.)	Related CSRs:	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***
2.2.9	Repairs and modifications to security-related physical components of a facility (e.g., hardware, walls, doors, and locks) are documented.	A maintenance tracking system should be implemented.	HIPAA 164.310(a)(2)(iv)
	Guidance: It is a good practice to keep an inventory of resources.	Related CSRs: 1.13.8	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***
2.2.10	All restricted areas used to protect sensitive information meet CMS criteria for secured area or security room, or provisions are made to store CMS sensitive information in appropriate security containers during non-working hours.	If Restricted Areas are used to protect sensitive information, review documentation establishing that each meets the specific CMS requirements for either a "Secured Area" or a "Security Room", or that provisions have been made to store CMS sensitive information in appropriate security containers during non-working hours.	IRS 1075 4.3@2.2 CMS Directed
	Guidance: Review BPSSM Section 4 for guidance.	Related CSRs: 1.7.1	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***

	General Requirement Control Technique	Protocol	Reference
2.2.11	CMS Sensitive information in any form is protected during non-working hours through a combination of a secured or locked perimeter, and a secured area or appropriate containerization.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used. 3. Review documentation establishing the protective methods and devices employed to protect sensitive information during non-working hours. Confirm use of one or more of the following controls: (1) secured or locked perimeter; (2) secured area; or (3) containerization.	IRS 1075 4.3@1.3 CMS Directed

Guidance: Review BPSSM Section 4 for guidance.

Related CSRs: 1.1.5, 1.7.1

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

2.2.12	Automated mechanisms are employed to control and audit that authorized-only access is permitted to media storage areas that are not protected by guard stations.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 MP-2 ARS MP-2.1 PISP 4.2.7.2

Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties.

Related CSRs: 2.8.3

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

2.2.13	Sensitive information (including tapes or cartridges) is placed in secure storage in a secure location, safe from unauthorized access. All containers, rooms, buildings, and facilities containing sensitive information are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.	1. Review facility security plan for procedures and policies for protection of sensitive information. 2. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of sensitive information data.	IRS 1075 4.3@19.2 IRS 1075 6.3@4 IRS 1075 4.3@19.4 CMS Directed

Guidance: Media controls should be planned for and designed to prevent the loss of confidentiality, integrity, or availability of sensitive information, including data or software, when stored outside the system.

Related CSRs: 6.4.3, 2.13.3

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

2.2.14	Sensitive information outside secured areas or security rooms during non-working hours is stored in one of the following: (1) metal lateral key-lock files; (2) metal lateral files equipped with lock bars on both sides and secured with security padlocks; (3) metal pull-drawer cabinets with center or off-center lock bars secured by security padlocks; or (4) key-lock "mini safes" properly mounted with appropriate key control.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements. 3. Review documentation supporting the contention that the required process is followed for storage of sensitive information.	IRS 1075 4.3@16.1 CMS Directed IRS 1075 4.3@16.3 IRS 1075 4.3@16.3.b IRS 1075 4.3@16.3.c IRS 1075 4.3@16.3.d IRS 1075 4.3@16.3.a IRS 1075 4.3@16.2

Guidance: Sensitive information kept within secured areas or security rooms during non-working hours can be stored in locked containers and do not require a security container. Otherwise, sensitive information must be stored in a security container or safe/vault. (See BPSSM Section 4 for additional information concerning these terms and requirements.)

Related CSRs:

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

	General Requirement Control Technique	Protocol	Reference
2.2.15	If safes and/or vaults are used to store CMS sensitive information outside secure or restricted areas, they comply with: (1) A safe is a GSA-approved container of Class I, IV, and V, or Underwriters Laboratories (UL) listings of TRTL-30, TXTL-60, or TRTL-60; (2) A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, and uses UL-approved vault doors, and meets GSA specifications.	Examine safe(s) or vault(s) for accompanying manufacturer documentation.	IRS 1075 4.3@18.1 CMS Directed IRS 1075 4.3@18.2

Guidance: Safes and/or vaults are not required for storage of sensitive information if provisions have been made to store CMS sensitive information in other appropriate security containers. However, if they are used, they must meet these GSA/UL requirements as stated in BPSSM Section 4.

Related CSRs:

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

	General Requirement Control Technique	Protocol	Reference
2.2.16	Locked containers must include lock mechanisms that use either a built-in key, or hasp and lock, and include the following features: (1) metal cabinet or box with riveted or welded seams, or (2) metal desks with locking drawers.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of containers to confirm inclusion of the required features.	IRS 1075 4.3@15.1 CMS Directed IRS 1075 4.3@15.2

Guidance: A locked container is any metal container which is locked and to which keys and combinations are controlled.

Related CSRs:

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

	General Requirement Control Technique	Protocol	Reference
2.2.17	Keys or other access devices are needed to enter the computer room and tape/media library. Unissued keys or other entry devices are secured.	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. 3. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.	FISCAM TAC-3.1.A.5 HIPAA 164.310(a)(2)(iii) FISCAM TAC-3.1.A.7

Guidance: Access to these areas should be limited to personnel with a legitimate need for access to perform their duties. Unissued keys and other entry devices should be stored in appropriate security containers.

Related CSRs: 2.8.3, 10.1.1

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

	General Requirement Control Technique	Protocol	Reference
2.2.18	All entry code combinations are changed periodically or when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.	1. Review audit data confirming consistent use of the required process. 2. Review documentation and logs for entry code changes. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 4.3@20.3 IRS 1075 4.3@20.6 HIPAA 164.308(a)(3)(ii)(C) FISCAM TAC-3.1.B.2

Guidance: Periodically changing entry codes prevents reentry by previous employees or visitors who might have knowledge of the entry code. There should be procedures for revoking physical access to controlled areas and removing user accounts when employees terminate employment or when others, such as contractors and vendors, no longer require access.

Related CSRs: 1.10.3, 2.9.17, 1.10.4

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

	General Requirement Control Technique	Protocol	Reference
2.2.19	Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.	Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.	HIPAA 164.310(c)

Guidance: Workstations are located in controlled access areas and are safeguarded from unauthorized access.

Related CSRs: 2.8.3, 3.6.3, 7.3.5, 7.3.2

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.2.20	Boot access to removable media drives is disabled when not explicitly required. Removable media drives are removed when not explicitly required. If a PC or laptop is not kept or used in a controlled environment, its system BIOS settings are locked and BIOS access is password protected.	1. Review system configuration logs. 2. Examine access audit logs. 3. Randomly validate BIOS access is protected on desktops. 4. Review documentation on authorized removable media.	ARS AC-CMS-1.CMS-3 ARS AC-CMS-1.CMS-2 ARS AC-CMS-1.CMS-1 CMS Directed
	Guidance:	Access to removable media drives should be tightly controlled. BIOS access should also be controlled.	Related CSRs: 1.3.12, 1.5.6
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
2.2.21	Physical ports (e.g., wiring closets, patch panels, etc.) are disabled when not in use.	Review documentation requiring the disabling of physical ports.	ARS PE-CMS-2.CMS-1 PISP 4.2.2.4
	Guidance:	Policy should exist which defines the physical ports that are required for operation.	Related CSRs: 2.1.2, 2.3.2, 5.1.4
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
2.2.22	Procedures are implemented to control access to software programs undergoing testing or revision.	Procedures are in place to protect CMS sensitive information during software testing and revisions.	HIPAA 164.310(a)(2)(iii)
	Guidance:	It is good practice to have an Security Test and Evaluation plan.	Related CSRs: 6.4.1
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
2.2.23	Responsibility is assigned and security procedures are implemented for bringing hardware and software into and out of the facility, as well as movement of these items within the facility, and for maintaining a record of those items.	Inspect documentation confirming that the required controls are implemented and consistently used.	HIPAA 164.310(d)(1) HIPAA 164.310(d)(2)(iii) NIST 800-53 PE-16 PISP 4.2.2.16
	Guidance:	The procedures for checking all hardware and software in to and out of the facility assist in maintaining an accurate inventory.	Related CSRs: 1.13.2, 5.4.2
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
2.2.24	Transmission and Storage of Data - Sensitive information may be stored on hard disk if the following condition has been met: The CMS Business Partner uses approved security access control devices (hardware/software) that receive regularly scheduled maintenance (including upgrades). Access control devices include: (1) password security; (2) audit trails/logs; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities. Data stored in the information system must be encrypted when residing in non-secure areas. Data stored in the information system must be encrypted when residing in non-secure areas.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documentation of approval and installation of the required devices. 3. Review documentation confirming that the access control devices include the required features. 4. Review audit data confirming accomplishment of the required maintenance and upgrades, 5. Review audit data confirming consistent use of the required control devices.	IRS 1075 4.7@6.1 CMS Directed IRS 1075 4.7@6.2 NIST 800-53 AC-3 ARS AC-3.CMS-5 PISP 4.3.2.3
	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: 5.9.5, 5.12.1, 3.6.1, 1.13.8, 1.13.9, 10.3.5
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
2.2.25	Sensitive information is locked in cabinets or sealed in packing cartons while in transit. Sensitive information material remains in the custody of a CMS or CMS Business Partner employee. Accountability is maintained during the move.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data supporting continuing use of the required processes.	IRS 1075 4.4 HIPAA 164.310(d)(2)(iii) NIST 800-53 MP-4 ARS MP-4.CMS-4 PISP 4.2.7.4
	Guidance:	The policies and procedures for protecting and transferring sensitive information materials with receipts ensure custody control and accountability during transfers.	Related CSRs: 1.3.3
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.2.26	Handling and Transporting Bulk Sensitive Information - Care is taken to safeguard sensitive information at all times. If hand carried between facilities, it is kept with an individual and protected from unauthorized disclosure. All shipments between facilities are documented on transmittal forms and monitored. All bulk shipments transmitted by the U.S. Postal Service, common carrier, or messenger service shall be sent in a sealed, opaque envelope, addressed by name and organization symbol, and marked "To be opened by addressee only."	1. Review sensitive information handling and transporting policies and procedures for control technique compliance. 2. Review sensitive information transmittal forms for accuracy and completeness. 3. Inspect a sample of sensitive information data media for labeling compliance with the requirement.	CMS Directed IRS 1075 4.5 IRS 1075 4.5@1.1 IRS 1075 4.5@1.2 IRS 1075 4.5@2.1 IRS 1075 4.5@2.2 IRS 1075 4.5@3.1

Guidance: These procedures apply ONLY to the routine and non-routine receipt, handling, and transporting of sensitive information BETWEEN FACILITIES. These requirements are NOT required for routine claims handling and mailings sent from business partners to Medicare recipients.

Related CSRs: 1.3.3, 2.5.5

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

	General Requirement Control Technique	Protocol	Reference
2.2.27	Delivery areas are isolated from restricted/controlled areas and are controlled to prevent unauthorized access. Delivery or removal of information system-related items (i.e., hardware, firmware, and software) is authorized by appropriate officials, and logs are maintained for the delivery and removal of information system-related items.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 PE-16 ARS PE-16 PISP 4.2.2.16

Guidance: Through the use of security controls and entry devices, limit access to personnel with a legitimate need for access to perform their duties.

Related CSRs: 5.9.8

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

	General Requirement Control Technique	Protocol	Reference
2.2.28	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. If wireless networks are used at alternate work sites, wireless base stations are placed away from outside walls to minimize transmission of data outside of the building.	1. Review relevant policies and procedures for inclusion and directed use of the required process by personnel working from their homes or alternate worksites. 2. Inspect documentation confirming that the required controls are implemented and consistently used.	IRS 1075 4.7@2 IRS 1075 4.7@3.1 IRS 1075 4.7@4.1 IRS 1075 4.7@5.1 CMS Directed IRS 1075 4.7@5.2 NIST 800-53 AC-20 NIST 800-53 PE-17 ARS AC-20.CMS-1 ARS PE-17.CMS-1 PISP 4.3.2.20 PISP 4.2.2.17

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

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

Related CSRs: 1.13.4, 1.13.5, 10.10.5

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

	General Requirement Control Technique	Protocol	Reference
2.2.29	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter restricted and other security areas after fire drills or other evacuation procedures.	1. Review written emergency procedures for inclusion of the required process. 2. Inspect a sample of audit data confirming use of the required process.	FISCAM TAC-3.1.A.8

Guidance: Re-entry access methods are used to provide appropriate controls at emergency exits.

Related CSRs: 2.8.1, 5.6.3, 5.1.5

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.2.30	Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.	1. If methods used to deny access to sensitive information by unauthorized personnel during working hours do not include use of Restricted Areas, Security Rooms, or Locked Rooms, then review documentation justifying use of alternative methods. 2. Review documentation establishing the methods employed to deny access to sensitive information from unauthorized personnel during working hours.	HIPAA 164.310(a)(2)(iii) IRS 1075 4.3@1.1 HIPAA 164.308(a)(3)(i)

Guidance: Procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.5.1, 2.5.4

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

2.2.31	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	1. Review audit data confirming consistent use of the required procedure. 2. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.	FISCAM TAC-3.1.B.3 NIST 800-53 MA-5 NIST 800-53 PE-7 ARS MA-5.0 PISP 4.2.5.5 PISP 4.2.2.7

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, 1.8.2, 1.9.9, 5.9.14

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

2.2.32	Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area 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 and reviewed by management at the end of each month. Automated mechanisms are employed to facilitate the maintenance and review of access logs. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of sign-in/sign-out registers to confirm collection of the required information. 3. Review a sample of audit data confirming compliance with the required register close out and review actions 4. Inspect a sample of audit data confirming monthly issue of a new AAL.	IRS 1075 4.3@4.1 HIPAA 164.308(a)(1)(ii)(D) HIPAA 164.310(a)(1) HIPAA 164.310(a)(2)(iii) IRS 1075 4.3@6 HIPAA 164.312(d) FISCAM TAC-3.1.B.1 IRS 1075 4.3@8.1 IRS 1075 4.3@8.4 IRS 1075 4.3@8.2 IRS 1075 4.3@4.2 IRS 1075 4.3@8.3 NIST 800-53 PE-2 NIST 800-53 PE-7 NIST 800-53 PE-8 ARS PE-7.1 ARS PE-8.1 ARS PE-8.0 ARS PE-2.0 PISP 4.2.2.2 PISP 4.2.2.7 PISP 4.2.2.8

Guidance: Persons other than regular authorized personnel may be granted access to sensitive areas or facilities, but these visitors are
controlled and not granted unrestricted access. Related CSRs: 1.9.9, 2.6.3

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

2.3 Access paths shall be identified.

2.3.1	An analysis of the logical access paths is performed whenever changes to the system are made.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.B

Guidance: It is important that all access paths (e.g., Internet, dial-in, telecommunications) be identified and controlled to eliminate "backdoor" paths. Related CSRs: 3.4.1, 4.5.1, 10.8.8

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

	General Requirement / Control Technique	Protocol	Reference
2.3.2	All access to proxies is denied, except for those hosts, ports, and services that are explicitly required.	1. Review list of hosts, ports, and services to which proxy access is granted. 2. Review the policy statement.	NIST 800-53 CM-7 NIST 800-53 SC-7 ARS CM-7.1 ARS SC-7.CMS-2 PISP 4.2.4.7 PISP 4.3.4.7

Guidance: Hosts, ports, and services that are required should be explicitly identified.

Related CSRs: 2.2.21, 10.2.8, 10.8.5

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

	General Requirement / Control Technique	Protocol	Reference
2.3.3	A trusted communications path is established between the user and the security functionality of the system.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review the trusted communications path.	NIST 800-53 SC-11 ARS SC-11 PISP 4.3.4.11

Guidance: It is important that only a trusted and controlled communications path be used when setting system security functionality.

Related CSRs: 10.10.1

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

2.4 Emergency and temporary access authorization shall be controlled.

	General Requirement / Control Technique	Protocol	Reference
2.4.1	Procedures are established (and implemented as needed) that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	1. Review documentation of the access control process to confirm inclusion of a procedure for emergency access. 2. Review documentation of the access control process to confirm inclusion of at least one of the required features.	HIPAA 164.312(a)(2)(ii) HIPAA 164.310(a)(1) HIPAA 164.312(a)(2)(i)

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: 5.2.6, 2.9.5, 5.6.3, 6.1.1

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

	General Requirement / Control Technique	Protocol	Reference
2.4.2	Emergency and temporary access authorizations are: (1) documented on standard forms and maintained on file; (2) approved by appropriate managers; (3) securely communicated to the security function; (4) automatically terminated after 15 minutes of no activity; and (5) automatically terminated after a predetermined period.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that all four specified elements of the required process is consistently used.	FISCAM TAC-2.2 NIST 800-53 AC-2 ARS AC-2.2 PISP 4.3.2.2

Guidance: As with normal access authorizations, emergency and temporary access should be approved and documented.

Related CSRs: 5.2.6, 2.2.1, 2.8.2, 6.1.1

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

General Requirement Control Technique	Protocol	Reference
2.5 Resource classifications and related criteria shall be established.		
2.5.1 To meet functional and assurance requirements, the operating security features of sensitive information systems must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to sensitive information.	1. Inspect documentation identifying systems that process sensitive information. 2. Review documentation establishing that all computers in all specified systems meet requirements in their implemented configuration. 3. Review documentation of the configuration management process used to assure that all systems remain in certified configurations.	IRS 1075 5.7@2.1 CMS Directed IRS 1075 5.7@2.4 IRS 1075 5.7@2.3 IRS 1075 5.7@2.2 NIST 800-53 SA-5 ARS SA-5.1 PISP 4.1.3.5

Guidance: The purpose of security is to support the function of the system, not to undermine it. Therefore, many aspects of the function of the system will produce related security requirements. Assurance documentation can address the security either for a system or for specific components. System-level documentation should describe the system's security requirements and how they have been implemented, including interrelationships among applications, the operating system, or networks. System-level documentation addresses more than just the operating system, the security system, and applications; it describes the system as integrated and implemented in a particular environment. Component documentation will generally be an off-the-shelf product, whereas the system designer or implementer will generally develop system documentation.

Related CSRs: 2.2.30, 1.9.4, 2.1.2

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

General Requirement Control Technique	Protocol	Reference
2.5.2 Every personnel position with access to CMS sensitive information processing is designated with a sensitivity level and risk designation, and the risk designations are reviewed and revised annually. Documentation is available to support the security and suitability standards for these personnel commensurate with their position sensitivity level and appropriate personnel investigation requirements.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample of personnel positions, inspect documentation establishing the associated sensitivity level.	CMS Directed NIST 800-53 PS-2 ARS PS-2.0 PISP 4.2.1.2

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, 1.10.2

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

General Requirement Control Technique	Protocol	Reference
2.5.3 Classifications and criteria have been established and communicated to resource owners.	1. Review policies specifying classification categories and related criteria to be used by resource owners in classifying their resources according to the need for protective controls. 2. Inspect audit data confirming that the required policy has been communicated to resource owners.	FISCAM TAC-1.1 PISP 4.2.1

Guidance: Policies and procedures specifying classification categories and related criteria are established in accordance with Section 4 of the BPSSM to help resource owners classify their resources according to their need for protection controls.

Related CSRs: 1.7.1, 2.7.1

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

General Requirement Control Technique	Protocol	Reference
2.5.4 Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation establishing that existing safeguards provide the required protections.	HIPAA 164.312(d) IRS 1075 6.3@8.a HIPAA 164.308(a)(3)(i) HIPAA 164.308(a)(3)(ii)(A) HIPAA 164.308(a)(4)(ii)(B) HIPAA 164.308(a)(4)(ii)(C)

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, 2.2.30, 2.7.2, 2.9.4

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

	General Requirement Control Technique	Protocol	Reference
2.5.5	Sensitive information is kept separate from other information to the maximum extent possible. If automated information labeling is utilized, information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs/requires special handling). If specific types of media or hardware components are exempted from labeling requirements, they remain within a secure environment and the exemption is authorized in writing by the Business Partner CIO, or his/her designated representative.	1. Review sensitive information handling procedures for inclusion of the required processes. 2. For a sample of media and devices containing sensitive information, inspect to confirm use of the required labels.	IRS 1075 5.3@1.1 IRS 1075 5.3@2.1 IRS 1075 5.3@3.1 IRS 1075 5.3@3.2 CMS Directed NIST 800-53 AC-16 NIST 800-53 MP-3 NIST 800-53 MP-4 ARS AC-16.CMS-1 ARS MP-3.0 PISP 4.3.2.16 PISP 4.2.7.3 PISP 4.2.7.4

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: 2.2.3, 1.3.13, 2.2.26, 1.13.7

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

2.5.6	Sensitive information system development documentation is available, including security mechanisms and implementation.	Inspect system design and test documentation for an explanation of security mechanisms and how they are implemented.	FISCAM TCC-1.1.1 NIST 800-53 SA-5 ARS SA-5.2 PISP 4.1.3.5

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

Related CSRs: 6.3.11

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

2.5.7	Sensitive information system documentation contains the test policy, test plan, test procedures, and retest procedures, and it describes how and what mechanisms were tested, and the results.	Review the sensitive information system documentation for inclusion of required test documentation.	FISCAM TCC-2.1.1 FISCAM TCC-2.1.4 FISCAM TCC-2.1.8

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: 6.3.8, 6.3.7

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

2.5.8	Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	CMS Directed IRS 1075 5.6@8

Guidance: The procedures are used to test the security system attributes.

Related CSRs: 1.12.1, 5.7.1

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

2.5.9	Security functions are isolated from non-security functions through the use of independent modules in a layered structured (minimizing interactions between layers of the design). Additionally, the security functions for enforcing access and information control are isolated and protected from other security functions and non-security functions.	1. Review documentation establishing that existing safeguards provide the required protections. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 SC-2 NIST 800-53 SC-3 ARS SC-3.3 ARS SC-3.2 ARS SC-3.4 ARS SC-3.5 ARS SC-3.1 PISP 4.3.4.3

Guidance: Security functions should be isolated from non-security functions through the use of information system partitions and domains. Separate execution domains (e.g. address space) should be maintained for each executing process. Hardware separation mechanisms should be employed to facilitate the isolation of security functions.

Related CSRs: 2.10.1

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

2.5.10 Users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. System resources shared between two or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

1. Review documentation establishing that existing safeguards provide the required protections.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

NIST 800-53 SC-4
ARS SC-4.0
HSPD-7 E(12)
PISP 4.3.4.4

Guidance: Policies and procedures should exist that address these control objectives.

Related CSRs:

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

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

2.6.1 Inappropriate or unusual activities or violations with security implications, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. Security personnel are notified and the identified unauthorized, unusual, and sensitive access activities are reported to management, investigated, and appropriate action is taken.

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

FISCAM TAC-4.2
NIST 800-53 AU-6
NIST 800-53 SI-4
ARS AU-6.2
ARS AU-6.CMS-3
ARS SI-4.CMS-1
PISP 4.3.3.6
PISP 4.2.6.4

Guidance: Audit functions should be activated to maintain critical audit trails and report unauthorized or unusual activity to the appropriate personnel.

Related CSRs: 7.1.1, 7.2.2, 7.3.4, 7.3.6, 8.1.1, 8.1.3, 8.1.2, 8.2.1, 8.2.2, 4.2.2, 3.1.1, 10.2.4, 2.9.10, 10.2.9, 10.2.6

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

2.6.2 Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.

1. Review documentation of the controls used to enforce this requirement.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

CMS Directed

Guidance: Audit trails are a mechanism that help managers maintain individual accountability. By advising computer operators that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.

Related CSRs: 3.6.5, 5.2.3

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

2.6.3 Procedures instruct supervisors: (1) to monitor the activities of visitors to the work area (including CMS Business Partner employees from other work areas); and (2) to ensure that functions of the unit are performed only by employees assigned to the unit. Supervisors shall have procedures for handling questionable activities.

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

CMS Directed

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

Related CSRs: 2.2.32

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

2.7 Owners of classified resources shall assign adequate classification to documentation and systems.

2.7.1 Resources are classified based on risk assessments. Classifications are documented and approved by an appropriate senior official, and are periodically reviewed.

1. Review resource classification documentation and compare to risk assessments.
2. Inspect audit data confirming that the required approval and review processes are consistently used.

FISCAM TAC-1.2
HSPD-7 F(19)(b)

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, 2.5.3, 1.8.5, 4.4.1, 1.12.2

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

2.7.2 Access to sensitive information is on a strictly need-to-know basis. Contractors evaluate the need for the sensitive information before the data is requested or disseminated.

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

IRS 1075 5.2@1.1
HIPAA 164.308(b)(1)
HIPAA 164.308(a)(4)(ii)(C)
IRS 1075 5.2@1.3
CMS Directed
HIPAA 164.308(a)(4)(i)
NIST 800-53 MP-4
ARS MP-4.CMS-4
PISP 4.2.7.4

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, 2.5.4, 2.9.4

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

2.8 Resource owners shall identify authorized users and the level of authorization.

2.8.1 Policy and procedures are implemented for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.

Review the appropriate documented policies and procedures for inclusion of the required rules.

HIPAA 164.312(a)(1)
HIPAA 164.312(e)(1)
HIPAA 164.308(a)(3)(i)

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: 2.2.29

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

2.8.2 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to the SSO. SSOs or their designated representative review access authorizations and discuss any questionable authorizations with resource owners.

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

FISCAM TAC-2.1.1
FISCAM TAC-2.1.4

Guidance: Policies and procedures should exist for authorizing access to information resources and for documenting such authorizations.

Related CSRs: 2.14.1, 2.2.1, 1.4.1, 2.4.2, 3.3.3

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

2.8.3 Authorization lists and controls for restricted areas, such as the computer room, tape library, and workstation rooms, are maintained. Authorization lists show the following information: (1) who is authorized access to restricted areas; (2) who is authorized to operate the equipment; (3) which workstations are authorized to access the computer and computer records; and (4) who may maintain operating systems, utilities, and operational versions of application programs.

1. By inspection, confirm that authorization lists include the required information.
2. Inspect audit data confirming continuing maintenance of authorization lists and access controls for restricted areas.

CMS Directed
NIST 800-53 PE-2
ARS PE-2.0
PISP 4.2.2.2

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: 6.4.2, 2.2.5, 2.2.19, 2.2.17, 2.2.12, 2.13.3

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

2.8.4 All changes to security profiles by SSO or designated representative are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect audit data confirming routine identification and investigation of unusual activity.
3. Review a selection of recent profile changes and activity logs.

FISCAM TAC-2.1.5
NIST 800-53 AU-6
ARS AU-6.CMS-6
PISP 4.3.3.6

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: 9.3.3, 3.1.1

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

General Requirement Control Technique	Protocol	Reference
2.8.5 The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a selection of users with dial-up access, review authorization and justification.	FISCAM TAC-2.1.3 NIST 800-53 AC-17 ARS AC-17.8

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, 5.9.12, 5.9.13

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

General Requirement Control Technique	Protocol	Reference
2.8.6 Owners periodically review access authorization listings and determine whether they remain appropriate.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TAC-2.1.2

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: 1.4.1, 2.2.1

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

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

General Requirement Control Technique	Protocol	Reference
2.9.1 If a CMS Business Partner is part of a larger organization, the Business Partner must implement policies and procedures that protect CMS sensitive information from unauthorized access by the larger organization.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Interview a sample of users to confirm the required understanding and access authorizations.	HIPAA 164.308(a)(4)(ii)(A)

Guidance: Review security policies and procedures for business partner access.

Related CSRs: 1.4.5

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

General Requirement Control Technique	Protocol	Reference
2.9.2 Public users (i.e., users who have not been authenticated) only have access to the extent necessary to accomplish mission objectives while preventing unauthorized access to sensitive information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Access selected personnel with access control responsibilities. 3. Examine system configuration settings to determine if the system allows users to perform certain actions without I&A.	NIST 800-53 AC-14 ARS AC-14.1 PISP 4.3.2.14

Guidance: Policies and procedures should exist that identify which specific user actions can be performed without I&A.

Related CSRs: 2.10.5, 3.2.3, 10.7.8, 10.8.5

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

General Requirement Control Technique	Protocol	Reference
2.9.3 User identification is required for any transaction that has information security implications.	1. Review helpdesk procedures. 2. Interview helpdesk personnel to verify understanding of requirement.	NIST 800-53 IA-2 ARS IA-CMS-1.CMS-1 ARS IA-2.CMS-1 PISP 4.3.1.2 PISP 4.3.1.8

Guidance: Help desk policy should require individual identification before transactions can be completed.

Related CSRs: 2.2.3, 7.3.3

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

	General Requirement Control Technique	Protocol	Reference
2.9.4	The use of passwords and access control measures are in place to identify who accessed protected information, limit that access to persons with a need-to-know, and prohibit the use of access scripts containing embedded passwords.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review Access Authorization Lists to confirm designation of all users allowed access to each separate security partition within the system (e.g. each platform root logon, each application relating to a unique separation of duties boundary, and each network device that supports direct logon). 3. Review documentation describing audit systems implemented to record all accesses, including access scripts, to protected information. 4. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description. 5. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing. 6. Inspect a sample of access audit data supporting continuing use to the required process.	HIPAA 164.312(e)(1) FISCAM TAC-3.2.A HIPAA 164.312(a)(1)
	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, 2.2.3, 2.5.4, 7.4.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.5	Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.	Review documentation establishing that authorization control exists, and includes the required feature.	HIPAA 164.308(a)(4)(ii)(B)
	Guidance: The mechanisms are used to authenticate users before granting them access permissions to the system or application.	Related CSRs: 2.4.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.6	Users maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others, and report lost items immediately.	1. Interview a sample of users to confirm the required understanding and device possession. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.8 NIST 800-53 IA-5
	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: 1.1.2	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.7	Passwords are distributed securely and users are informed not to reveal their passwords to anyone (e.g., social engineering). A process is in place for handling lost and compromised passwords.	1. Review the policies and procedures for distributing passwords. 2. Review the policies and procedures for handling lost and compromised passwords.	NIST 800-53 IA-5 ARS IA-5.0 PISP 4.3.1.5
	Guidance: Users take reasonable measures to safeguard passwords, including not loaning or sharing passwords with others, and reporting lost or compromised passwords immediately.	Related CSRs: 1.1.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

2.9.8 Entity authentication (the corroboration that an entity is the one claimed) exists and includes a unique user identifier and automatic logoff after a predetermined amount of time (normally 15 minutes). It also includes multifactor authentication (password combined with token, password with biometric, etc.).

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

HIPAA 164.312(a)(2)(iii)
HIPAA 164.312(d)
HIPAA 164.312(a)(2)(i)
NIST 800-53 IA-2
NIST 800-53 IA-4
ARS IA-2.1
ARS IA-2.CMS-1
PISP 4.3.1.2

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

Related CSRs: 10.8.2, 10.10.1

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

2.9.9 For password-based authentication, passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) not displayed when entered; (4) changed every 60 days, when an individual changes positions, or when security is breached; (5) not displayed when entered; (6) at least 8 characters in length; (7) must include at least one number, one upper and lower case character, and one special character; and (8) prohibited from reuse for at least 6 generations. The use of dictionary names or words as passwords is prohibited.

1. Interview users.
2. Review security software password parameters.
3. Observe users keying in passwords.
4. Attempt to log on without a valid password. Make repeated attempts to guess passwords.
5. Assess procedures for generating and communicating passwords to users.
6. Review pertinent policies and procedures.

FISCAM TAC-3.2.A.2
FISCAM TAC-3.2.A.1
CMS Directed
HIPAA 164.308(a)(5)(ii)(D)
FISCAM TAC-3.2.A.4
NIST 800-53 IA-5
NIST 800-53 IA-6
ARS IA-6.0
ARS IA-5.0
ARS IA-2.CMS-2
NIST 800-53 IA-2
PISP 4.3.1.2
PISP 4.3.1.5
PISP 4.3.1.6

Guidance: Policies and procedures should exist that implement these minimum password requirements. The use of alphanumeric passwords reduces the risk that an unauthorized user could gain access to a system by using a computer to try dictionary words or names until the password is guessed.

Related CSRs: 7.3.3, 10.10.1, 1.1.1, 3.6.2

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

2.9.10 Systems are configured to disable access for 15 minutes after 3 failed logon attempts. User account lockout results from 3 consecutive disable cycles, and requires an administrator-level reset to restore access to the user account.

1. Review security software password parameters.
2. Review pertinent policies and procedures.
3. Observe the system directed action in response to four invalid access attempts, confirming that the action is consistent with the documented policy.

FISCAM TAC-3.2.A.5
NIST 800-53 AC-7
ARS AC-7.0
PISP 4.3.2.7

Guidance: Procedures should exist for resetting logon features after three failed attempts. To prevent guessing of passwords, attempts to log onto the system with invalid passwords should be limited.

Related CSRs: 2.6.1, 7.3.6

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

	General Requirement Control Technique	Protocol	Reference
2.9.11	When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) authentication is provided through UserID and password encryption for use over public telephone lines; (2) standard access is provided through a toll-free number and through local telephone numbers to local data facilities; and (3) both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards should have both identification and authentication features and provide for data encryption.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the specified controls for all dialup access to systems handling sensitive information. (Controls for packet switched network access are covered in other control techniques.) 3. Review audit data, including spot inspections, confirming that all the specified controls are applied to all dialup access. This includes review of all devices having potential access to sensitive information that are equipped with modems. 4. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.	IRS 1075 5.8@5.1 IRS 1075 5.8@5.2.a FISCAM TAC-3.2.E.1 IRS 1075 5.8@5.2.c IRS 1075 5.8@5.2.d IRS 1075 5.8@5.2 NIST 800-53 AC-17 ARS AC-17.8
	Guidance: The entity should have cost-effective physical and logical controls in place for protecting systems accessed remotely. The purpose of this CSR is to prevent unauthorized access or disclosure of PHI by implementing controls that reflect industry security standards. Without authentication, the system cannot verify the provider or supplier is who they claim to be. Without encryption, the system cannot protect the data while in transit. If the PHI is under the control of the business partner, it is expected they will provide reasonable protection. Where the business partner considers the cost is excessive, they should seek alternative controls that will be more cost effective. For example; if modems are already implemented without encryption, the business partner may propose software encryption as an alternate control. In the event the business partner is unable to find less expensive alternatives, they need to provide a cost to meet this CSR in a Safeguard. CMS will then consider the cost and associated risk in funding these solutions over time.	Related CSRs:	3.6.1, 3.6.3, 10.8.2, 10.10.3, 10.10.4
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***	
2.9.12	In a session, inactivity at any workstation during any 15 minute period shall cause the system to automatically terminate (disable) workstation access to the system. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords are utilized where supported by existing operating systems.	1. Inspect a sample of workstations running each type of operating system in use to confirm that the required process is in use. 2. Review configuration documentation supported implementation of the required feature.	FISCAM TAC-3.2.C.3 CMS Directed HIPAA 164.310(b) NIST 800-53 AC-11 NIST 800-53 SC-10 ARS AC-11.0 ARS SC-10.0 ARS SC-10.CMS-1 ARS SC-10.CMS-2 ARS AC-12.0 NIST 800-53 AC-12 PISP 4.3.2.11 PISP 4.3.2.12 PISP 4.3.4.10
	Guidance: Workstation and desktop time-outs and password protected screen savers are important access controls used to prevent unauthorized users from accessing the system using the logged-on users credentials.	Related CSRs:	10.10.1
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC***	☑ ***Dmerc*** ☑ ***DC***	☑ ***CWF*** ☑ ***COB***	

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.9.13	Limits on the number of concurrent sessions for any user are established and enforced. The information system is configured to notify the user, upon successful log-on, of the date and time of the last log-on, and the number of unsuccessful log-on attempts since the last successful log-on.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review configuration documentation supporting implementation of the required feature. 3. Interview a sample of users to confirm the required process is in use.	CMS Directed NIST 800-53 AC-9 NIST 800-53 AC-10 ARS AC-9.0 ARS AC-10.0 PISP 4.3.2.9 PISP 4.3.2.10
	Guidance: Establishing and enforcing concurrent session limits assists in preventing users from having unnecessary sessions open.		Related CSRs:
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.14	The information system provides feedback to users during an attempted authentication that does not reveal authentication information (e.g., UserID, password length, token) to the user that would compromise the system authentication mechanism.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review configuration documentation supporting implementation of the required feature. 3. Interview a sample of users to confirm the required process is in use.	CMS Directed NIST 800-53 IA-6 ARS IA-6.0 PISP 4.3.1.6
	Guidance: Keeping the system authentication feedback information confidential prevents the authentication mechanisms from being revealed to outside users. For example, revealing the UserID and password length can be of great assistance to a hacker trying to gain access to the system.		Related CSRs: 10.2.10
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.15	System administrators maintain separate user accounts with separate UserIDs and passwords; one exclusively for standard user functions (e.g., Internet, e-mail, etc.) and one for system administration activities. These UserIDs are not shared with anyone.	1. Ensure that System Administrators have unique UserID when performing admin functions. 2. Interview System Administrators regarding their UserIDs 3. Review usage reports to establish activity.	NIST 800-53 IA-4 ARS IA-4.CMS-1 PISP 4.3.1.4
	Guidance: Available procedures define the usage of the unique UserIDs.		Related CSRs: 2.1.4, 2.1.3
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.16	Unique and separate administrator accounts based on the users' roles and responsibilities are used for administrator versus non-administrator activities. Where multiple administrators are employed, maintain a limited number who have full access. Centralized control of user access administrator functions is implemented.	1. Ensure that System Administrators have unique UserID when performing admin functions. 2. Interview System Administrators regarding their UserIDs.	NIST 800-53 AC-2 NIST 800-53 AC-5 ARS AC-2.CMS-3 ARS AC-2.CMS-2 ARS AC-5.CMS-2 PISP 4.3.2.2 PISP 4.3.2.5
	Guidance: The use of unique and separate accounts helps to ensure that administrative activities are kept separate from non-administrative activities.		Related CSRs: 2.1.3, 2.1.4
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
2.9.17	Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	1. Review pertinent policies and procedures. 2. Review documentation of such comparisons. 3. Interview security managers. 4. Make comparison using audit software.	FISCAM TAC-3.2.A.6 NIST 800-53 AC-2 ARS AC-2.1 PISP 4.3.2.2
	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: 1.10.3, 2.2.18, 1.10.4
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.9.18	Inactive user accounts are monitored and automatically removed when not needed or after 30 days.	1. Review a sample of audit data confirming continued operation of the required control. 2. Review documentation describing how the required control is implemented.	FISCAM TAC-3.2.C.4 NIST 800-53 AC-2 NIST 800-53 CA-7 NIST 800-53 IA-4 ARS AC-2.3 ARS IA-4.0 PISP 4.3.2.2 PISP 4.3.1.4

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: 1.10.3

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

2.9.19	Vendor-supplied passwords are replaced immediately.	1. For a sample of applications and network devices, attempt to log on using common vendor-supplied passwords. These default passwords are usually documented in the associated manuals. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.3

Guidance: Vendor supplied passwords are known by every hacker and they are usually the first passwords tried by hackers.

Related CSRs: 3.6.2, 10.10.1

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

2.9.20	A callback capability with re-authentication is used to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a UserID and password, and enters the network through the standard authentication process. Access to such systems is authorized and logged. UserIDs assigned to vendors are renewed on a six-month basis.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Examine the system configuration to determine if a callback capability is implemented when the MDCN cannot be used.	NIST 800-53 AC-17 ARS AC-17.CMS-3 PISP 4.3.2.17

Guidance: Policies and procedures should exist that specify the callback measures

Related CSRs: 3.6.2

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

2.10 Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure.

2.10.1	Security software is used to restrict access. Only authorized information security personnel have access to system security functions deployed in hardware, software, and firmware.	1. Review documentation describing the security software in use for restriction of access to data files and software programs. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of security software parameters that limit access to the security software to security administrators.	FISCAM TAC-3.2.C.1 FISCAM TAC-3.2.C.2 NIST 800-53 AC-3 ARS AC-3.1 PISP 4.3.2.3

Guidance: The most commonly used means of restricting access to data files and software programs is through the use of access control software, also referred to as security software. Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted.

Related CSRs: 3.6.4, 3.6.5, 2.5.9

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

2.10.2 Security administration personnel set parameters in security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files and operating system files. Standardized naming conventions are used for resources.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Perform penetration testing by attempting to access and browse computer resources.
3. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
4. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.
5. Review documentation describing the standardized naming conventions in use for resources.

FISCAM TAC-3.2.C.5
FISCAM TAC-3.2.C.6

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: 6.4.1, 2.1.6, 3.6.5, 6.4.2, 6.8.1, 7.1.2, 7.2.1

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

2.10.3 Modification of data is restricted to authorized employees.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect the Access Authorization List(s) identifying employees who are authorized to update data.
3. Inspect a sample of audit data confirming that the required process is consistently used
4. Review documentation of the control used to restrict of data updating to authorized employees.

CMS Directed

Guidance: Logical access controls provide a technical means of controlling what information users can access (in accordance with relevant policy), the programs they can run, and the modifications they can make. Logical access controls may be implemented internally to the computer system being protected or may be implemented in external devices.

Related CSRs: 7.4.1

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

2.10.4 Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, uncatalog, scratch, and rename a file.

1. Review documentation of the process used to provide the specified control over routines that modify the status of a file.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.

CMS Directed

Guidance: Utilities for file access and related processing need controls in place.

Related CSRs: 7.4.1

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

Category: ***Access Control***

	General Requirement Control Technique	Protocol	Reference
2.10.5	Operating system controls are configured to disable public “read” and “write” access to all system files, objects, and directories. Operating system controls are configured to disable public “read” access to files, objects, and directories that contain sensitive information.	1. Validate security program system setup or rules (RAC-F/ACF2/TopSecret) or access setup in other operating systems. 2. Examine access in system audit logs.	NIST 800-53 AC-3 NIST 800-53 SC-14 ARS AC-3.CMS-4 ARS SC-14.CMS-1 ARS AC-6.CMS-5 NIST 800-53 AC-6

Guidance: It is important that the OS controls are implemented to disable public read and write access to sensitive information.

Related CSRs: 1.9.3, 2.9.2

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

2.11 Logical controls shall be implemented for databases and DBMS software.

2.11.1	Access and changes to DBMS software are controlled. Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	1. Review the controls protecting DBMS software. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.D.3 FISCAM TAC-3.2.D.4 HIPAA 164.310(a)(2)(iii)

Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. In addition, DBMS software changes should be protected from unauthorized changes through the use of logical access controls.

Related CSRs: 6.5.1, 6.6.1, 3.4.1

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

2.11.2	The use of database management system (DBMS) utilities is limited. DBMS and data dictionary controls have been implemented that: (1) restrict access to data files at the logical data view, field and field-value level; (2) implement row and column-level access controls; (3) control access to the data dictionary using security profiles and passwords; (4) maintain audit trails/logs that allow monitoring of changes to the data dictionary; and (5) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List for DBMS utilities to confirm access is limited to those personnel have an operational requirement for access.	FISCAM TAC-3.2.D.2 NIST 800-53 AC-3 NIST 800-53 AC-6 NIST 800-53 CA-7 ARS AC-3.CMS-3 ARS AC-6.CMS-4 PISP 4.3.2.3 PISP 4.3.2.6

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: 2.1.4

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

2.12 Sensitive material shall be protected.

2.12.1	Access to sensitive information is limited to those who are authorized by law or regulation. Physical and systemic barriers are reviewed/reported. Assessments are conducted of facility security features.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	IRS 1075 6.3@5 NIST 800-53 PE-3 ARS PE-3.CMS-1 PISP 4.2.2.3

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: 2.5.4, 1.12.6, 2.7.2

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

2.12.2	Medicare data is not released to outside personnel unless the personnel are authorized to receive the data and their identity is verified.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	CMS Directed

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

Related CSRs: 1.3.2, 1.3.7, 10.3.2, 10.3.1

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

2.13 Suspicious access activity shall be investigated and appropriate action taken.

2.13.1 SSOs investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken and violations are summarized and reported to senior management.

1. Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
2. Interview senior management and personnel responsible for summarizing violations.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM TAC-4.3.1
FISCAM TAC-4.3.3
FISCAM TAC-4.3.2

Guidance: Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations should be investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur, repair any damage. The seriousness of the issue should determine what disciplinary actions might be taken. A good approach is to tie these violations/accidents into performance evaluations.
The frequency and magnitude of security violations and corrective actions taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the entity's operations, and any need for additional controls.

Related CSRs: 7.1.1, 7.2.2, 7.3.4, 7.3.6, 8.1.1, 8.1.3, 8.1.2, 8.2.1, 8.2.2, 3.1.1

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

2.13.2 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.

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

FISCAM TAC-4.3.4

Guidance: Once it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur and repair any damage that has been done.

Related CSRs: 7.3.4, 7.3.6, 8.1.1, 8.1.3, 8.1.2, 8.2.1, 8.2.2, 3.1.2, 3.1.1, 3.4.1

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

2.13.3 Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.

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

IRS 1075 3.2@2.4
CMS Directed

Guidance: The process of inventorying and documenting missing tapes containing sensitive information should be integrated into the normal business processes of the organization.

Related CSRs: 2.2.13, 2.8.3, 6.4.3

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

2.14 Owners shall determine disposition and sharing of data.

2.14.1 Standard forms are used to document approval for archiving, deleting, and sharing data files.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect standard approval forms.

FISCAM TAC-2.3.1

Guidance: A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard forms should be used and maintained on file to document the users' approvals.

Related CSRs: 1.3.7, 2.8.2

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

	General Requirement Control Technique	Protocol	Reference
2.14.2	Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.	Examine documents authorizing file sharing and file sharing agreements.	FISCAM TAC-2.3.2 HSPD-7 H(25)(b)

Guidance: Resource owners should determine if, with whom, and by what means information resources can be shared. When files are shared with other entities, it is important that (1) data owners understand the related risks and approve such sharing, and (2) receiving entities understand the sensitivity of the data involved and safeguard the data accordingly. This should normally require a written agreement prior to the sharing of sensitive information.

Related CSRs: 1.11.3, 1.11.4

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

3. *System Software*

3.1 Inappropriate or unusual activity shall be investigated and appropriate actions taken.

	General Requirement Control Technique	Protocol	Reference
3.1.1	Measures define investigation of inappropriate or unusual activity and the appropriate actions to be taken.	Review system operational policies and guidelines.	FISCAM TSS-2.2.2 NIST 800-53 AU-6 ARS AU-6.CMS-3 PISP 4.3.3.6

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, 8.1.3, 8.1.2, 8.2.1, 8.2.2, 2.6.1, 2.13.1, 2.13.2, 2.8.4, 4.2.2

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

	General Requirement Control Technique	Protocol	Reference
3.1.2	Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Determine when the last management review was conducted, and analyze their review regarding the intended functioning of software monitoring control techniques and controlling risk.	FISCAM TSS-2.2.4 NIST 800-53 CA-7 ARS CA-7.CMS-1 PISP 4.1.4.7

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: 6.3.14, 1.5.4, 1.8.1, 1.8.8, 1.8.5, 1.8.2, 1.8.3, 2.13.2, 4.4.1

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

	General Requirement Control Technique	Protocol	Reference
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 UserIDs for performing privileged and normal activities? - Are the login privileges for highly privileged accounts available only from console and terminals situated within the console room ? - Is the audit trail maintained of activities conducted by highly privileged users? How long is it preserved?	FISCAM TSS-2.2.1

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

Related CSRs: 1.8.2, 3.3.3, 4.1.1, 4.3.1, 4.6.1, 10.7.8

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

3.1.4 Systems programmers' activities are monitored and reviewed.

1. Determine that system programmer supervisors are supervising and monitoring their staff.
2. Review documentation supporting the supervising and monitoring of systems programmers' activities.
3. System Programmer and/or System Administrators need supervisor rights to make modifications. These personnel need additional controls in place to prevent misuse of these rights.

FISCAM TSS-2.2.3

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: 4.2.2, 4.4.2, 3.2.2

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

3.1.5 Systems support alarm features to provide immediate notification of predefined events.

1. Review security plan to determine use of audit logs and alarms set points.
2. Review audit logs.

HIPAA 164.312(b)

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

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.4, 4.1.1, 9.3.1, 9.3.5, 9.7.1, 2.1.13

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

3.2 Policies and techniques shall be implemented for using and monitoring system utilities.

3.2.1 Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.

1. Verify that the appropriate responsibilities have been defined.
2. Interview systems programmers regarding their responsibilities.

FISCAM TSS-2.1.2

Guidance: Security training is adjusted to the level of the system programmer's responsibilities. The FISCAM defines a system programmer as someone who develops and maintains system software and related utilities.

Related CSRs: 1.1.3

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

3.2.2 Responsibilities for monitoring use are defined and understood by technical management. Procedures for using and monitoring use of system software utilities are implemented and are up-to-date.

1. Verify that the appropriate responsibilities are defined.
2. Interview technical management regarding their responsibilities.
3. Interview management and systems personnel.
4. Verify the existence and current version of the appropriate policies and procedures.

FISCAM TSS-2.1.3
FISCAM TSS-2.1.1

Guidance: Security training is adjusted to the level of the technical management's responsibilities. It is a good practice to identify access for various programs and utilities, monitoring, and written policies and procedures. As part of the System Security Plan, policies and procedures for using and monitoring the use of system software utilities should be defined and documented.

Related CSRs: 1.1.3, 3.1.4, 4.1.4, 1.4.8

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

3.2.3 Privilege restrictions are enabled to limit public and employee access to administrator tools, scripts, and utilities. The use of sensitive system tools, scripts, and utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).

1. Determine whether logging occurs and what information is logged.
2. Review logs.
3. Using security software reports, determine who can access the logging files.

FISCAM TSS-2.1.4
NIST 800-53 AC-3
ARS AC-3.CMS-3
PISP 4.3.2.3

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: 1.9.2, 9.6.6, 2.1.4, 2.9.2, 10.7.8

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

3.3 Access authorizations shall be appropriately limited.

3.3.1 Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.

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

FISCAM TSS-1.1.2

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

Related CSRs: 1.1.5

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

3.3.2 Procedures for restricting access to systems software are implemented and are up-to-date. Justification and management approval for access to systems software is documented and retained.

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. Interview system manager and security administrator.
5. Review pertinent policies and procedures.

FISCAM TSS-1.1.1
FISCAM TSS-1.1.3

Guidance: Access to system software is restricted to a few system programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly. The SSO normally maintains an approved Access Control Listing (ACL) for all systems that process or transmit sensitive data. The individual's supervisor provides justification and approval to the SSO. The ACL is part of the System Security Profile.

Related CSRs: 1.9.2, 1.9.9

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

3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.

Determine the last time the access capabilities of system programmers were reviewed.

FISCAM TSS-1.1.4

Guidance: Security skill needs are accurately identified and included in job descriptions. The duties from the job description should be compared to the SSO's security access list and the security audit logs. If these functions do not match then management should take corrective action(s). The review memo should be provided to the SSO for inclusion in the System Security Profile.

Related CSRs: 3.1.3, 4.6.3, 4.6.1, 2.8.2

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

Category: ***System Software***

General Requirement

Control Technique | **Protocol** | **Reference**

3.4 Installation of system software shall be documented and reviewed.

3.4.1 Installation of all system software is logged to establish an audit trail/log and is reviewed by data center management.

1. Interview data center management about their role in reviewing system software installations.
2. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.

FISCAM TSS-3.2.4

Guidance: A good process for monitoring and documenting migration of system software is in the change management process for the organization.

Related CSRs: 9.7.1, 9.8.1, 9.8.2, 9.8.3, 6.5.1, 2.3.1, 2.11.1, 2.13.2, 4.7.5, 6.3.6, 6.3.12, 6.3.14, 6.6.1, 6.7.2, 6.8.2, 10.7.2, 10.10.1

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

3.4.2 Migration of tested-and-approved system software to production use is performed by an independent library control group.

Interview management, systems programmers, and library controls personnel, and determine who migrates approved system software to production libraries, and whether versions are removed from production libraries.

FISCAM TSS-3.2.2

Guidance: A good process for monitoring and documenting the migration of system software is in the change management process for the organization.

Related CSRs: 6.8.1, 4.7.5

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

3.4.3 Vendor-supplied system software includes software documentation and is supported by the vendor.

Interview system software personnel concerning a selection of system software and documentation, and determine the extent to which the operating version of the system software is currently supported by the vendor.

FISCAM TSS-3.2.5

Guidance: A good approach is to include vendor maintenance with the purchase of the software.

Related CSRs: 5.8.1, 6.3.13, 4.1.5

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

3.4.4 Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.

1. Interview management and systems programmers about scheduling and giving advance notices when system software is installed.
2. Review recent installations and determine whether scheduling and advance notification did occur.
3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.

FISCAM TSS-3.2.1

Guidance: If possible, a good approach to scheduling major installations of system software is during off hours. This creates minimal impact on operations and provides time to back out the installation if errors occur. Notification can be provided several days in advance via email.

Related CSRs: 5.9.4

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

	Control Technique	Protocol	Reference
3.4.5	All system software is current and has current and complete documentation. Outdated versions of system software are removed from production libraries.	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. 3. Review supporting documentation from a few system software migrations and the removal of outdated versions from production libraries.	FISCAM TSS-3.2.6 FISCAM TSS-3.2.3

Guidance: An automated version tracking system can assist with tracking the current version of software and the software's documentation. Outdated versions are kept in a library other than the production library. In order to prevent redundant execution of older versions, they should be deleted from production and moved elsewhere. Storage for outdated versions may be part of the Contingency Plan reconstitution efforts.

Related CSRs: 1.9.2

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

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

	Control Technique	Protocol	Reference
3.5.1	New system components and system software versions or products and modifications to existing system software receive proper authorization, are supported by a change request document, are tested, and the test results are approved before implementation.	1. Determine the procedures used to test and approve system components and software prior to its implementation. 2. Select a few recent system component and software changes and review audit data confirming that the specified process was followed. 3. Review procedures used to control and approve emergency changes. 4. Select some emergency changes to system components and software, and test whether the indicated procedures were used. 5. Determine what authorizations and documentation are required prior to initiating system software changes. 6. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.	FISCAM TSS-3.1.4 FISCAM TSS-3.1.3

Guidance: This should be documented and provided in the Change management process. Change management standards, proper controls, processes, and procedures will provide for appropriate testing prior to implementation. A preformatted change request process provides efficiency and assists in the accuracy of the change tracking processes.

Related CSRs: 5.7.4, 6.6.1, 6.7.2, 4.7.5, 10.7.5

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

	Control Technique	Protocol	Reference
3.5.2	Controls exist and are up-to-date for identifying, selecting, installing and modifying system software. Controls include a mission/business impact analysis, including the training required to implement the controls; an analysis of costs and benefits; and consideration of the impact on processing reliability and security.	1. Interview management and systems personnel. 2. Verify that policies and procedures are current, and contain the required information. 3. Review the mission/business impact analysis documentation.	FISCAM TSS-3.1.1 NIST 800-53 CM-4 PISP 4.2.4.4

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

Related CSRs: 1.9.2, 1.4.1, 1.8.2, 4.1.3

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

Category: ***System Software***

	General Requirement Control Technique	Protocol	Reference
3.5.3	Procedures are implemented for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.	1. Review procedures for identifying and documenting system software problems. 2. Interview management and systems programmers. 3. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.	FISCAM TSS-3.1.2

Guidance: A good approach is to automate the software problem tracking processes. Monthly tracking reviews will assist in controlling any issues.

Related CSRs: 1.9.2

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

3.5.4	Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.	Verify the existence of checkpoint and restart capabilities.	CMS Directed

Guidance: Checkpoints and restart capabilities on jobs will assist in meeting performance goals.

Related CSRs: 4.7.5

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

3.5.5	Procedures are implemented for controlling emergency changes. These procedures include: (1) authorizing and documenting emergency changes as they occur, (2) reporting the changes for management review, and (3) review of the changes by an independent IT supervisor.	1. Interview an independent IT supervisor who has previously reviewed changes. 2. Verify the existence of emergency change procedures. 3. Interview system managers.	FISCAM TSS-3.1.5 NIST 800-53 CM-3 PISP 4.2.4.3

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: 5.7.2, 6.6.1, 1.9.2

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

3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.

3.6.1	All accesses to system software files are logged by automated logging facilities.	Review sample accesses to system software files to confirm automated logging facilities.	FISCAM TSS-1.2.2

Guidance: This is part of the application and system access controls. Included could be an alerting process when an automated notification process can identify suspicious logging or file changes occur.

Related CSRs: 2.2.24, 2.9.11, 10.7.7

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

3.6.2	All vendor-supplied default logins, passwords, and security parameters have been removed, disabled or reinitialized to more secure settings.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Test for default presence using vendor standard IDs and passwords.	FISCAM TSS-1.2.3 NIST 800-53 AC-2 NIST 800-53 IA-5 ARS AC-2.CMS-1 PISP 4.3.2.2

Guidance: Disabling default passwords and logins, and changing default security settings to more secure settings should be part of enhancing security (hardening) process when new software or systems are installed.

Related CSRs: 2.9.19, 1.9.2, 10.10.1, 2.9.9, 2.9.20

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

3.6.3	Remote access to the system master console is restricted. Physical and logical controls provide security over all workstations that are set up as master consoles.	1. Determine what terminals are set up as master consoles and what controls exist over them. 2. Test to determine if the master console can be accessed, or if other terminals can be used to mimic the master console and take control of the system.	FISCAM TSS-1.2.4 NIST 800-53 AC-17 ARS AC-17.8

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: 1.9.2, 2.2.19, 2.9.11, 10.10.2

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

Category: ***System Software***

	General Requirement Control Technique	Protocol	Reference
3.6.4	Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access is generally limited to primary and backup systems programmers.	1. Obtain a list of all system software on test and production libraries used by the entity. 2. Verify that access control software restricts access to system software. 3. Using security software reports, determine who has access to system software files, security software, and logging files. Reports should be generated by the auditor, or at least in the presence of the auditor. 4. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.	FISCAM TSS-1.2.2 HIPAA 164.310(a)(2)(iii) NIST 800-53 AC-5 ARS AC-5.CMS-2 PISP 4.3.2.5

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, 10.7.7, 4.6.1

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

3.6.5	The operating system is configured to prevent circumvention of the security software and application controls.	1. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods. 2. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.	FISCAM TSS-1.2.1 NIST 800-53 AC-5 ARS AC-5.1

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, 2.2.4, 2.6.2, 10.7.7

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

3.6.6	The operating system's operational status and restart integrity is protected during and after shutdowns.	1. Interview the system manager. 2. Verify the protection of the operating system during and after shutdowns.	CMS Directed NIST 800-53 SI-6 ARS SI-6.0 PISP 4.2.6.6

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: 5.2.8

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

3.6.7	Secure information system recovery and reconstitution includes, but is not limited to: (1) resetting all system parameters (either default or organization-established), (2) reinstalling patches, (3) reestablishing configuration settings, (4) reinstalling application and system software, and (5) fully testing the system. A full recovery and reconstitution of the information system is performed as part of the Contingency Plan testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify through testing or procedure reviews that system defaults are reset after being restored from a backup.	NIST 800-53 CP-10 NIST 800-53 IA-5 ARS CP-10.1 ARS CP-10.0 HSPD-7 G(22)(i) PISP 4.2.3.10

Guidance: Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, and application and system software is reinstalled.

Related CSRs: 5.2.1

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

4. *Segregation of Duties*

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

Control Technique	Protocol	Reference
4.1.1 Detailed, written instructions exist to guide personnel in performing their duties. Computer operator manuals provide guidance on system startup and shutdown procedures, emergency procedures, system and job status reporting, and operator-prohibited activities. Application-specific manuals provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.	1. Determine that the required operator and security manuals exist, and that they provide the required documentation. 2. Determine that documents are understood and adhered to by staff.	FISCAM TSD-3.1.2 NIST 800-53 SI-11 ARS SI-11.0 HSPD-7 G(22)(i) PISP 4.2.6.11

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: 9.1.1, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.3, 3.1.5, 2.1.10, 4.2.3, 5.6.3

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

Control Technique	Protocol	Reference
4.1.2 Duties in critical mission functions or sensitive control, financial functions, and information system support functions are divided among separate individuals to ensure least privileged and individual accountability.	1. Interview supervisors in the critical and sensitive control and financial areas. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	CMS Directed ARS AC-5.CMS-3 NIST 800-53 AC-5 PISP 4.3.2.5

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

Related CSRs: 4.3.1, 4.7.2

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

Control Technique	Protocol	Reference
4.1.3 The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing use of the specified approval process.	CMS Directed NIST 800-53 CM-4 PISP 4.2.4.4

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

Related CSRs: 3.5.2, 10.7.6

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

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

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

Related CSRs: 9.1.1, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5, 3.2.2

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

Control Technique	Protocol	Reference
4.1.5 Application-run manuals provide instruction on operating specific applications, including in-house applications.	1. Inspect run manuals for inclusion of the required instructions. 2. Employees demonstrate that documentation is understood and adhered to.	FISCAM TSD-3.1.3

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: 3.4.3, 6.3.13

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

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

4.2.1 Personnel are provided adequate supervision and review, including each shift of computer operations.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data confirming continuing supervision and review in accordance with the documented process.

FISCAM TSD-3.2.1
NIST 800-53 AC-13
ARS AC-13.1

Guidance: Supervision and review of personnel activities assure that these activities are performed in accordance with prescribed procedures, mistakes are corrected, and computers are used for authorized purposes.

Related CSRs: 1.4.1, 4.7.4, 7.6.1

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

4.2.2 All operator activities on the computer system are recorded on an automated history log. Supervisors routinely review the history log and investigate any abnormalities.

1. Determine by review that an automated history log exists on each computer system, and that they record all operator activities.
2. Determine, by review supervisor's job description that this is included in the job description.
3. Review history log for signatures indicating supervisory review.
4. Inspect a sample of documentation of the supervisor's investigative process.
5. Interview supervisors to confirm that supervisors routinely review history log.

FISCAM TSD-3.2.3
FISCAM TSD-3.2.2

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

Related CSRs: 2.1.1, 2.6.1, 3.1.4, 7.3.4, 7.3.6, 8.1.1, 8.1.3, 8.1.2, 8.2.2, 3.1.1

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

4.2.3 System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.

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

FISCAM TSD-3.2.4
NIST 800-53 SI-6
ARS SI-6.0
NIST 800-53 AC-13
ARS AC-13.CMS-2
PISP 4.3.2.13
PISP 4.2.6.6

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

Related CSRs: 4.1.1, 10.2.1

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

4.3 Job descriptions shall be documented.

4.3.1 Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.

1. Review documentation establishing that existing documented job descriptions meet segregation of duty principles.
2. Inspect the effective dates of position descriptions to confirm that they are current.
3. Confirm by interview of the incumbents that documented job descriptions match actual current responsibilities and duties.

FISCAM TSD-1.2.1
NIST 800-53 AT-3
PISP 4.2.9.3

Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.

Related CSRs: 3.1.3, 4.1.2

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

Category: ***Segregation of Duties***

General Requirement 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 TSD-1.2.2

Guidance: HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department. Related CSRs: 5.1.9

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

4.4 Management shall review job duties for effectiveness of control techniques.

General Requirement 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 TSD-2.2.2

Guidance: A good approach is a documented management review on an annual basis. Related CSRs: 3.1.2, 2.7.1, 4.7.1

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

General Requirement 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 TSD-2.2.1

Guidance: A periodic employee performance review could be used to demonstrate compliance. Related CSRs: 3.1.4

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

4.5 Physical and logical access controls shall be established.

General Requirement Control Technique	Protocol	Reference
4.5.1 Physical and logical access controls restrict employees to authorized actions, based upon organizational and individual job responsibilities.	Review documentation establishing now physical and logical access controls accomplish the specified restriction.	FISCAM TSD-2.1 CMS Directed NIST 800-53 AC-5 ARS AC-5.CMS-2 PISP 4.3.2.5

Guidance: This can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities. Related CSRs: 2.3.1

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

4.6 Employees shall understand their security duties and responsibilities.

General Requirement Control Technique	Protocol	Reference
4.6.1 Security skill needs are accurately identified and included in job descriptions. All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	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. 3. Interview employees to confirm that their job descriptions match their understanding of their duties and responsibilities, and that they carry out those responsibilities in accordance with their job descriptions.	FISCAM TSD-1.3.1 FISCAM TSP-4.2.1

Guidance: The SSO should work in conjunction with the HR department on job description updates. Employees should have access to their job descriptions and discuss during their performance evaluations. Related CSRs: 3.1.3, 3.3.3, 3.6.4

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

Category: ***Segregation of Duties***

General Requirement
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 TSD-1.3.2

Guidance: Senior management is responsible for assuring that employees understand their responsibilities. Related CSRs: 1.2.2

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

4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.

1. Review documented procedures identifying responsibilities for restricting access by job position in key operating and programming activities to confirm that these responsibilities are clearly defined.
2. Interview a sample of personnel identified as having the specified responsibilities to confirm that the responsibilities assigned are clearly understood and followed.
3. Employees demonstrate that documentation is understood and adhered to.

FISCAM TSD-1.3.3
NIST 800-53 AC-5
ARS AC-5.CMS-6
PISP 4.3.2.5

Guidance: A good approach is to develop a matrix identifying resources in relation to organizational access and job title. Related CSRs: 3.3.3

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

4.7 Incompatible duties shall be identified and policies implemented to segregate these duties.

4.7.1 Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

Review approval controls.

FISCAM TSD-1.1.4

Guidance: Compensating controls should be documented. Related CSRs: 4.4.1

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

4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through practices and organizational divisions. No individual has complete control over incompatible transaction processing functions.

1. Review the required analyses for inclusion of the specified elements.
2. Confirm by review that the required analyses reflect current operations.
3. Confirm through inspection that the required policies and procedures exist and are consistent with current operations.

FISCAM TSD-1.1.3
FISCAM TSD-1.1.1

Guidance: Establish independent organizational groups with defined functions. Functions and related tasks performed by each unit should be documented. Policies are documented, communicated, and enforced. Related CSRs: 4.1.2

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

4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.

1. Review documentation of process design establishing the specified separation of duties.
2. Confirm through interview, observation, and review of job descriptions for a sample of personnel, that these separation of duties requirements are met.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM TSD-1.1.5
NIST 800-53 SI-9
ARS SI-9
PISP 4.2.6.9

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: 1.5.1

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

4.7.4 Day-to-day operating procedures for the data center are adequately documented and implemented, and prohibited actions are identified.

Confirm by review that documented operating procedures meet the required criteria.

FISCAM TSD-1.1.6

Guidance: Documentation should be reviewed periodically and updated as needed.

Related CSRs: 4.2.1

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

4.7.5 Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) testing functions (i.e., user acceptance, quality assurance, information security); (6) library management/change management; (7) computer operations; (8) production control and scheduling; (9) data control; (10) data security; (11) data administration; and (12) network administration.

1. Review the agency organization chart showing IS functions and assigned personnel.
2. Interview selected personnel and determine whether functions are appropriately segregated.
3. Review relevant alternative or backup assignments and determine whether the proper segregation of duties is maintained.
4. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.

FISCAM TSD-1.1.2
NIST 800-53 AC-5
ARS AC-5.CMS-4
ARS AC-5.CMS-6
PISP 4.3.2.5

Guidance: Manuals and job descriptions include support functions of each individual.

Related CSRs: 3.4.1, 3.4.2, 3.5.4, 3.5.1

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

5. *Service Continuity*

5.1 Adequate environmental controls shall be implemented.

5.1.1 Environmental controls are monitored and periodically tested. Levels of alert are evaluated and prescribed guidelines for each alert level are evaluated. When necessary, response procedures are implemented and monitored, management is alerted of possible loss of service and/or media, damage is reported, remedial action is provided, and the Contingency Plan is implemented.

1. Review the test plans for future tests.
2. Review test policies.
3. Review documentation supporting recent tests of environmental controls.

FISCAM TSC-2.2.6

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

Related CSRs: 5.7.1

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

5.1.2 Controls have been identified to sufficiently mitigate identified risks and other disasters, such as floods, earthquakes, fire, etc.

1. Review the risk assessment plan for consideration of the specified potential risks.
2. Review documentation of efforts to identify additional risks specific to the region, area, or facility.
3. Review documentation of risk mitigation planning covering all identified risks.
4. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.

FISCAM TSC-2.2.2

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: 1.8.2, 2.2.29, 5.6.2

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

Category: ***Service Continuity***

	General Requirement Control Technique	Protocol	Reference
5.1.3	An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down. Where necessary to maintain an operational capability, a redundant and parallel power cabling path, or a long-term alternate power supply is provided for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	1. Review facility documentation confirming installation of an uninterruptible power system (UPS). 2. Review design and test data supporting the capacity of the system to support the facility technical load long enough to allow shut down with lose of no more that transactions in progress at the time primary power is lost. 3. Review documentation supporting existence of periodic test, and preventive maintenance consistent with system specifications. 4. Review policies and procedures for orderly shut down of the system within the time allowed by the available UPS capacity. 5. Interview a sample of operations personnel for familiarity with the orderly shut down process and applicable documented procedures. 6. Review documentation supporting periodic test of the orderly shut down process. 7. Observe that secondary power supplies exists.	FISCAM TSC-2.2.5 NIST 800-53 PE-11 ARS PE-11.1 ARS PE-9.1 NIST 800-53 PE-9 PISP 4.2.2.9 PISP 4.2.2.11

Guidance: The facility managers should periodically verify the current computing power load and auxiliary requirements for change.

Related CSRs: 5.9.7, 5.10.1

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

5.1.4	Electric power distribution, heating plants, water, sewage, and other utilities are periodically reviewed for risk of failure. Information system power equipment and power cabling are protected from damage and destruction. Only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.	1. Review relevant policies and procedures for inclusion of the required process. 2. Review documentation supporting recent reviews of environmental controls.	NIST 800-53 PE-9 ARS PE-9.CMS-1 HSPD-7 G(22)(i) PISP 4.2.2.9

Guidance: There should be a process for the testing of the environmental controls and periodic reviews for risk of failure.

Related CSRs: 2.2.21, 10.1.2, 5.9.14

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

5.1.5	A master power switch or emergency cut-off switch is implemented, maintained, and prominently marked and protected by a cover for Data Centers, server, and mainframe rooms. Emergency lighting systems that activate automatically in the event of a power outage or disruption and that cover emergency exits and evacuation routes are implemented and maintained.	1. Review relevant policies and procedures for inclusion of the required process. 2. Observe the master power or emergency cut-off switch. 3. Observe the emergency lighting systems.	NIST 800-53 PE-10 NIST 800-53 PE-12 ARS PE-10.CMS-1 ARS PE-12 PISP 4.2.2.10 PISP 4.2.2.12

Guidance: Policies and procedures should exist that address these control objectives.

Related CSRs: 2.2.29

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

5.1.6	Redundancy exists in the air cooling system. Acceptable temperature and humidity levels are maintained and monitored, and specific control alarms within facilities containing information systems are monitored. Levels of alert are evaluated and prescribed guidelines for each alert level are evaluated. When necessary, management is alerted of possible loss of service and/or media, damage is reported, remedial action is provided, and the Contingency Plan is implemented.	1. Review facility design documentation confirming air cooling system redundancy. 2. Review maintenance records confirming primary and redundancy systems are operational. 3. Observe demonstrations of operation of primary and redundant cooling systems. 4. Review policy and procedures relevant to operation and maintenance of primary and redundancy air cooling systems	FISCAM TSC-2.2.3 NIST 800-53 PE-14 ARS PE-14.CMS-1 ARS PE-14.CMS-2 ARS PE-14.CMS-3 PISP 4.2.2.14

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

Related CSRs: 5.2.1

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

Category: ***Service Continuity***

General Requirement
Control Technique **Protocol** **Reference**

5.1.7 Fire suppression and detection devices that activate automatically or can be activated in the event of a fire (e.g., smoke detectors, fire extinguishers, and sprinkler systems) have been installed and are working. The fire suppression and detection devices are configured to automatically notify emergency responders and the organization upon activation.

1. Review facility drawings and other documentation documenting types and locations of the specified devices.
2. Review documentation of periodic inspections and maintenance of the specified devices and related systems to assure they are fully operational.
3. Review documentation supporting the qualifications of personnel inspecting and maintaining the specified devices and systems.
4. Observe that fire extinguishers, smoke detectors and sprinkler systems are in place and appear to be in working order.

FISCAM TSC-2.2.1
NIST 800-53 PE-13
ARS PE-13.1
ARS PE-13.2
PISP 4.2.2.13

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

Related CSRs: 5.6.3

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

5.1.8 Building plumbing lines are known and do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known. Automated mechanisms are implemented to close shutoff valves automatically in the event of a significant water leak.

1. Examine facility maintenance records for history of water damage.
2. Interview site managers for knowledge of potential pumping related hazards and familiarity with mitigation procedures.
3. Interview a sample of operations staff to confirm familiarity with mitigation procedures for potential plumbing related problems.
4. Observe the operation, location, maintenance, and access to the air cooling systems condensate drains.
5. Observe whether water can enter through the computer room ceiling or pipes are running through the facility, and that there are water detectors on the floor.
6. Review relevant procedures for inclusion mitigation measures for any potential plumbing related problems.
7. Review the current risk assessment to confirm investigation of the potential for plumbing related problems, and review risk mitigation plans for any such risks identified.

FISCAM TSC-2.2.4
NIST 800-53 PE-15
ARS PE-15.1
PISP 4.2.2.15

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

Related CSRs: 5.6.2

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

5.1.9 Any behavior that may damage computer equipment is prohibited. Power surge protection is implemented for all computer equipment.

1. Review the risk assessment for identification of potentially hazardous employee activities.
2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment.
3. Review job descriptions to ensure there is guidance contained relative to destructive behavior.

FISCAM TSC-2.2.7
ARS PE-CMS-1.CMS-1
PISP 4.2.2.11

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

Related CSRs: 4.3.2

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

5.2 A Contingency Plan shall be documented in accordance with the CMS Business Partners Systems Security Manual.

5.2.1	Contingency Plans consist of all components listed in the CMS Business Partners Systems Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.	1. Review Appendix B of the Business Partners Systems Security Manual. 2. Verify through inspection that the Contingency Plan includes the specified elements.	CMS Directed HIPAA 164.310(d)(1) FISCAM TSC-3.1.1 HIPAA 164.308(a)(7)(ii)(C) HIPAA 164.308(a)(7)(ii)(D) HIPAA 164.308(a)(7)(ii)(E) HIPAA 164.308(a)(7)(i) HIPAA 164.308(a)(7)(ii)(A) NIST 800-53 CP-2 NIST 800-53 CP-3 NIST 800-53 CP-5 ARS CP-2.1 ARS CP-2.0 ARS CP-5.0 ARS CP-3.1 PISP 4.2.3.2 PISP 4.2.3.3 PISP 4.2.3.5

Guidance: A business partner Contingency Plan contains the topics described in Appendix B of the Business Partners Systems Security Manual. Development of the Contingency Plan is coordinated with parties responsible for related plans, such as the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan and Incident Response Plan.

Related CSRs: 5.3.1, 5.4.3, 5.4.5, 5.5.1, 5.6.1, 5.8.1, 3.6.7, 5.1.6

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

5.2.2	Management, the SSO, and key affected parties approve Contingency Plans.	1. Verify through inspection that all Contingency Plans have been approved by management, SSO, and key affected parties. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-3.1.1 CMS Directed NIST 800-53 CP-2 NIST 800-53 CP-4 PISP 4.2.3.2 PISP 4.2.3.4

Guidance: It is important that the Contingency Plan be reviewed and approved by persons that are knowledgeable about the systems and environment so that nothing is missed in the plan.

Related CSRs: 5.7.2

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

5.2.3	Management and the SSO are able to show how the organization responds to specific disasters/disruptions to: (1) protect lives, (2) limit damage, (3) protect sensitive data, (4) circumvent safeguards according to established bypass procedures, and (5) minimize the impact on Medicare operations.	1. Review documentation, CCTV tapes or other recordings. 2. Determine through interview that system manager(s) and the SSO can explain how the organization covers each of the specified requirements through its response to specific disasters/disruptions.	FISCAM TSC-3.1.1 CMS Directed

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, 5.10.1, 2.6.2

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

5.2.4	The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.	1. Review test reports. 2. Verify through inspection that the contingency plan identifies the specified interfaces.	CMS Directed

Guidance: Critical interfaces should be tested when the contingency plan is exercised.

Related CSRs: 5.3.1

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

	General Requirement Control Technique	Protocol	Reference
5.2.5	The Contingency Plan clearly assigns responsibilities for recovery and provides for backup personnel so that it can be implemented independent of specific individuals.	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. 4. Review the Contingency Plan to confirm clear identification of specific responsibilities for all elements of recovery.	FISCAM TSC-3.1.1 FISCAM TSC-3.1.2 NIST 800-53 CP-2 PISP 4.2.3.2

Guidance: Ensure that individuals have been assigned to all the responsibilities that need to be executed during a contingency. Refer to Appendix B of the BPSSM.

Related CSRs: 3.6.4, 4.3.1, 4.6.1, 5.6.1, 5.8.1, 5.10.2

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

5.2.6	The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.	Review the Contingency Plan emergency response procedures for inclusion of the required provision.	CMS Directed HIPAA 164.308(a)(7)(ii)(C)

Guidance: Ensure that this immediate entry action has been practiced during exercises and training.

Related CSRs: 2.4.1, 2.4.2, 5.6.1, 5.6.3, 2.2.5

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

5.2.7	Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency Plans are re-evaluated before proposed changes are approved.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming that contingency plans have been reevaluated before any proposed major modifications were approved.	CMS Directed

Guidance: Change control management should provide for updates to the Contingency Plan.

Related CSRs: 5.7.2

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

5.2.8	Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.	1. Review documentation supporting the contention that existing contingency plans protect storage media from improper modification in the event of system failure. 2. Review documentation describing use of installed security and backup capabilities to reduce the potential for data loss and/or modification during a system failure. 3. Review documentation describing use of software procedures to reduce the potential for data loss and/or modification during a system failure.	CMS Directed HSPD-7 G(22)(i)

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, 6.4.2, 7.2.2, 9.8.1, 5.11.2, 9.3.3

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

5.2.9 User departments have developed adequate manual processing procedures for use until automated operations are restored.

1. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation.
2. Review the contingency plan for identification of the specified manual procedures.
3. Inspect the required manual procedures for consistency with the contingency plan.
4. Interview the relevant process managers to confirm familiarity with the required procedures.
5. Review test reports to determine that manual procedures have been tested, at least on a sample basis.

FISCAM TSC-3.1.3

Guidance: Determine that the manual procedures have been tested. Refer to Appendix B of the BPSSM.

Related CSRs: 1.8.2

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

5.3 Critical data and operations shall be identified and prioritized.

5.3.1 A list of critical applications, operations and data has been documented that: (1) prioritizes data and operations; (2) is approved by senior program managers; and (3) reflects current conditions.

1. Verify by inspection that the required, prioritized list has been prepared.
2. Verify by inspection that the list is approved by senior management.
3. Review documentation supporting the contention that the list reflects current conditions.
4. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM TSC-1.1
HIPAA 164.308(a)(7)(ii)(E)

Guidance: It is important to know what critical data and operations are needed to continue critical functions in an emergency.

Related CSRs: 1.8.3, 2.1.5, 5.4.1, 5.8.1, 5.2.4

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

5.4 Data and program backup procedures shall be implemented.

5.4.1 The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.

1. Observe the initiation of delivery of critical data from the primary site to the off-site facility.
2. Review the Contingency Plan to verify that it contains the specified elements.
3. Review records of data backups.

HIPAA 164.310(d)(1)
CMS Directed
HIPAA 164.308(a)(7)(ii)(A)

Guidance: Refer to Appendix B of the BPSSM.

Related CSRs: 5.11.1

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

5.4.2 A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.

An inventory of all equipment and software should be maintained, including the location and person responsible.

HIPAA 164.310(d)(2)(iv)

Guidance: A record should be use to track the movement all resources.

Related CSRs: 2.2.23

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

Category: ***Service Continuity***

	General Requirement Control Technique	Protocol	Reference
5.4.3	System and application documentation are maintained at the off-site storage location.	1. Interview persons at the primary site who are responsible for storing documents off-site. 2. Review documentation supporting maintenance of the required off-site storage. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TSC-2.1.2 ARS CP-7.0 NIST 800-53 CP-7 PISP 4.2.3.7
	Guidance:	Current systems and applications documentation should be available off-site in case the primary processing site is disabled.	Related CSRs: 5.7.3
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.4.4	The backup storage and alternate processing sites are identified in the Contingency Plan, and are geographically removed from the primary site(s) and protected by environmental controls and physical access controls. The backup storage and alternate processing sites are located at least 100 miles from the primary processing site.	1. By inspection, verify that the backup storage and alternate processing sites are consistent with available documentation. 2. Review documentation confirming that the backup storage and alternate processing sites meet the stated requirements.	FISCAM TSC-2.1.3 NIST 800-53 CP-6 NIST 800-53 CP-7 ARS CP-6.1 ARS CP-7.1 PISP 4.2.3.6 PISP 4.2.3.7
	Guidance:	It should be verified that the backup and alternate processing sites are geographically removed from the primary site and are protected by environmental and physical access controls.	Related CSRs: 5.11.2, 5.10.3
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.4.5	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged. Backup information is tested for media reliability and information integrity after each backup. Select backup information is used to restore information systems as part of the Contingency Plan testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent operation of the required rotation. 3. Verify by inspection the location of specific backup files. 4. Review documentation confirming successful periodic test of the ability to recover using backup files.	FISCAM TSC-2.1.1 HIPAA 164.308(a)(7)(ii)(B) NIST 800-53 CP-9 ARS CP-9.1 ARS CP-9.2 ARS CP-9.0 PISP 4.2.3.9
	Guidance:	Offsite backup files should be current to the point that operations would not be delayed or disrupted if the data or software were suddenly put into operation.	Related CSRs: 5.11.1, 5.9.7
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.4.6	Incremental backups are performed daily, and full backups are performed weekly. Three generations of backups are stored off site. Both off-site and on-site backups are logged with name, date, time, and action. Backup copies of the operating system and other critical information system software are stored at a separate facility or in a fire-rated container that is not collocated with operational software.	1. Review backup logs. 2. Inspect off-site backups.	NIST 800-53 CP-9 NIST 800-53 MP-4 ARS CP-9.3 ARS MP-4.CMS-1 ARS MP-4.CMS-2 PISP 4.2.3.9 PISP 4.2.7.4
	Guidance:	Off-site backup files should be current such that operations would not be delayed or disrupted beyond acceptable time limits in the event it becomes necessary to operate using the backup data or software.	Related CSRs: 1.3.10
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.5	Emergency processing priorities shall be established.		
5.5.1	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.	FISCAM TSC-1.3 HIPAA 164.308(a)(7)(ii)(C)
	Guidance:	Processing priorities should exist for all critical functions and processes to be accomplished during an emergency. These should be periodically reviewed for accuracy.	Related CSRs: 5.3.1, 5.6.3
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

General Requirement Control Technique	Protocol	Reference
5.6 Management and staff shall be trained to respond to emergencies.		
5.6.1 Employees have received training and understand their emergency roles and responsibilities. Simulated events are incorporated into contingency training to facilitate effective response by personnel in crisis situations. Automated mechanisms are employed to provide thorough and realistic training environments.	1. Interview a sample of employees to confirm their understanding of their roles in emergency response procedures. 2. Review training records to confirm required training has been conducted, and is consistent with the current procedures. 3. Review training plans for future training in emergency actions.	FISCAM TSC-2.3.1 NIST 800-53 CP-3 ARS CP-3.1 ARS CP-3.2 PISP 4.2.3.3

Guidance: There should be evidence that the employees have periodically received training relative to what to do in an emergency.

Related CSRs: 5.7.1

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

General Requirement Control Technique	Protocol	Reference
5.6.2 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.	1. Review training records to confirm that the required training has been delivered periodically. 2. Review training plans for future training in emergency actions.	FISCAM TSC-2.3.2 NIST 800-53 CP-3 ARS CP-3.1

Guidance: These are procedures primarily for staff and management working in a data processing center environment.

Related CSRs: 5.1.8, 1.6.4

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

General Requirement Control Technique	Protocol	Reference
5.6.3 Training in emergency procedures is conducted at least once a year and emergency procedures are periodically tested.	1. Verify the emergency procedures are dealt with in the COOP. 2. By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review documentation confirming completion of the required testing. 5. Review future test plans to ensure that the emergency procedures are scheduled to be properly tested. 6. Interview data center staff.	FISCAM TSC-2.3.4 FISCAM TSC-2.3.3 HIPAA 164.308(a)(7)(ii)(C) CMS Directed HIPAA 164.308(a)(7)(ii)(D) HIPAA 164.308(a)(7)(i)

Guidance: Emergency procedures should be defined in a procedure manual as part of the Contingency Plan and training performed annually. A record should be maintained that verifies that the training took place. Procedures for use during an emergency situation should be tested annually, or whenever major changes are made to the system environment. Refer to Appendix B of the BPSSM.

Related CSRs: 5.2.6, 5.5.1, 5.7.1, 2.2.29, 2.4.1, 4.1.1, 6.1.1, 5.1.7

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

5.7 The Contingency Plan shall be annually reviewed and tested.

5.7.1 The current Contingency Plan is executable and tested annually using a combination of tabletop exercises and operational tests under conditions that simulate an emergency or a disaster. Automated mechanisms are employed to more thoroughly and effectively test the contingency plan. The Contingency Plan is tested at the alternate processing site to evaluate the site's capabilities to support contingency operations. Testing of the contingency plan is coordinated with parties responsible for related plans, such as: (1) Business Continuity Plan, (2) Disaster Recovery Plan, (3) Continuity of Operations Plan, (4) Business Recovery Plan, and (5) Incident Response Plan.

1. Review documentation of annual conduct of the required test.
2. Review documentation describing how the testing conditions simulate an emergency or disaster.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Review test plans for upcoming contingency plan testing, including lessons learned from the previous testing.

FISCAM TSC-4.1
CMS Directed
HIPAA 164.308(a)(7)(ii)(D)
NIST 800-53 CP-4
ARS CP-4.1
ARS CP-4.2
ARS CP-4.3
ARS CP-5.0
NIST 800-53 CP-5
PISP 4.2.3.4
PISP 4.2.3.5

Guidance: It is advisable to conduct "live tests" of critical system processes to ensure they will function in an emergency.

Related CSRs: 5.6.3, 2.5.8, 5.6.1

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

5.7.2 Contingency Plans and associated documentation are reviewed and, if required, updated whenever new operations are planned or new safeguards contemplated. Contingency Plans must be updated minimally at least every 3 years. The Disaster Recovery Plan is current and executable, and it is tested once per year or when a major change is made to ensure proper functionality.

1. Review the current Contingency Plan to confirm it is updated as required.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

FISCAM TSC-3.1.1
CMS Directed
NIST 800-53 CP-4
NIST 800-53 CP-5
ARS CP-4.0
ARS CP-5.0
ARS CP-CMS-1.1
PISP 4.2.3.4
PISP 4.2.3.5
PISP 4.2.3.11

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: 1.9.9, 1.12.3, 3.5.5, 6.3.14, 5.2.7

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

5.7.3 Several copies of the current Contingency Plan are securely stored off-site at different locations, including homes of key staff members. It is reviewed once a year, reassessed and, if appropriate, revised to reflect changes in hardware, software and personnel.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review audit data supporting consistent annual review, reassessment, and appropriate revision of the contingency plan as specified.
3. Review documentation confirming the required off-site distribution and storage.

FISCAM TSC-3.1.4
FISCAM TSC-3.1.1
FISCAM TSC-3.1.5
CMS Directed
NIST 800-53 CP-2
NIST 800-53 CP-5
PISP 4.2.3.2
PISP 4.2.3.5

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

Related CSRs: 5.4.3, 5.9.4

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

5.7.4 Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review distribution records or interview senior management to ensure that they received the latest contingency plan test results and lessons learned information.

FISCAM TSC-4.2.1
NIST 800-53 CP-4
PISP 4.2.3.4

Guidance: Senior management should be informed in a timely manner of contingency plan test results and lessons learned so that they can direct appropriate actions to modify the plan or change test plans and procedures.

Related CSRs: 3.5.1

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

5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documents establishing that the contingency plan and related agreements are adjusted as specified.

FISCAM TSC-4.2.2
HIPAA 164.308(a)(7)(ii)(D)
NIST 800-53 CP-4
NIST 800-53 CP-5
ARS CP-4.0
PISP 4.2.3.4
PISP 4.2.3.5

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: 5.10.4, 1.11.5

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

5.8 Resources supporting critical operations shall be identified.

5.8.1 Key resources supporting critical and sensitive operations are identified and documented. Types of key resources identified include: (1) computer hardware; (2) computer software; (3) computer supplies; (4) system documentation; (5) telecommunications; (6) office facilities and supplies; and (7) human resources.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect documents identifying resources supporting critical and sensitive operations for inclusion of the specified resource types.

FISCAM TSC-1.2
NIST 800-53 CP-7
ARS CP-7.0
HSPD-7 D(8)
HSPD-7 E(12)
HSPD-7 F(19)(c)
HSPD-7 G(24)
HSPD-7 H(25)(a)
HSPD-7 J(27)(a)
HSPD-7 J(27)(b)
PISP 4.2.3.7

Guidance: It is important that resources needed to support critical and sensitive operations during an emergency and recovery time periods be documented for availability to all concerned persons, and that they be reviewed for currency whenever the contingency plan is to be tested.

Related CSRs: 5.3.1, 2.1.5, 5.4.1, 5.9.7, 5.2.5, 5.10.4, 3.4.3

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

5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.

5.9.1 Goals are established by senior management for the availability of data processing and on-line services. Senior management periodically: (1) reviews and compares the service performance achieved with the goals; and (2) surveys user departments to see if their needs are being met.

1. Interview users.
2. Review documentation confirming establishment of the required goals.
3. Review relevant policies and procedures for inclusion and directed use of the required process.
4. Review the performance records to ensure the goals are clearly stated in writing.

FISCAM TSC-2.4.9
FISCAM TSC-2.4.6

Guidance: Reasonable data processing goals should be set by management to guide the maintenance and problem analysis relative to hardware performance and availability. 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: 1.11.5, 10.2.9, 10.2.11

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

5.9.2 Records are maintained on the actual hardware performance in meeting service schedules.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect the required records.

FISCAM TSC-2.4.7

Guidance: Records should be kept for all critical hardware components in the system, such as mainframe, server, disc unit, tape unit, controllers, front end processors, and operations consoles and workstations.

Related CSRs: 1.11.5, 10.2.9

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

Category: ***Service Continuity***

General Requirement
Control Technique | **Protocol** | **Reference**

5.9.3 Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.

1. Review records of past advanced notifications.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.

FISCAM TSC-2.4.11

Guidance: Notice of at least 2 days should be given to users relative to hardware changes.

Related CSRs: 5.7.3, 10.7.2

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

5.9.4 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.

FISCAM TSC-2.4.10

Guidance: Any changes to hardware equipment or software should be carefully reviewed, tested, and a schedule created for implementation of the changes. Peak workload periods should be avoided for implementation. Vendor supplied specifications normally prescribe the frequency and type of preventative maintenance to be performed.

Related CSRs: 1.9.4, 5.7.3, 6.3.13, 10.7.2, 6.6.1, 3.4.4

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

5.9.5 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.

FISCAM TSC-2.4.4

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

Related CSRs: 2.2.24

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

5.9.6 Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.

1. Inspect hardware maintenance schedules
2. Review documentation supporting the contention that the hardware maintenance schedule complies with vendor specifications.
3. Review maintenance records to confirm completion of hardware maintenance in accordance with the schedule.
4. Review documentation supporting the contention that the manner of performing maintenance minimizes the impact of maintenance on operations.

FISCAM TSC-2.4.2
NIST 800-53 MA-2
ARS MA-2.2
PISP 4.2.5.2

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

Related CSRs:

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

	General Requirement Control Technique	Protocol	Reference
5.9.7	Maintenance support and spare parts is used to provide a high level of system availability for critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within 24 hours of failure.	1. Review documentation confirming availability of spare or backup hardware for support of applications designated as critical or sensitive. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review operations and maintenance documentation to confirm that levels of available backup or spare hardware have been sufficient to support system availability objectives.	FISCAM TSC-2.4.5 NIST 800-53 MA-6 ARS MA-6.0 PISP 4.2.5.6
	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: 5.4.5, 5.4.4, 5.10.1, 5.11.1, 5.11.2	
	□ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.8	Regular and unscheduled hardware maintenance performed is documented. The maintenance log for each system includes: (1) date and time of maintenance; (2) name of the individual performing the maintenance; (3) name of escort, if applicable; (4) description of the maintenance performed; and (5) list of equipment removed or replaced (including identification numbers, if applicable).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance documentation for conformance with the documented procedures.	FISCAM TSC-2.4.3 NIST 800-53 MA-2 ARS MA-2.1 PISP 4.2.5.2
	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: 1.8.2, 1.9.9, 2.2.27	
	□ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.9	Measures and automated mechanisms are employed to ensure that maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and complete, is up-to-date, accurate, and readily available. Automated mechanisms are employed to ensure only authorized personnel use maintenance tools. Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information, or maintenance personnel are supervised during the performance of maintenance activities when they do not have the needed access authorizations.	1. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them. 2. Review documentation supporting the contention that the required policies and procedures are up-to-date. 3. Inspect maintenance policies and procedures.	FISCAM TSC-2.4.1 NIST 800-53 MA-2 NIST 800-53 MA-5 ARS MA-2.2 ARS MA-5.0 PISP 4.2.5.2 PISP 4.2.5.5
	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: 1.9.4, 1.4.1, 1.8.2	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.10	The use of system maintenance tools is approved, controlled, and monitored; and the tools are maintained on an on-going basis. All maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel are inspected for obvious improper modifications. The use of remote diagnostic tools is documented in the SSP. All media containing diagnostic programs is checked for malicious code before the media is used in the system.	1. Review documentation supporting the contention that the required policies and procedures are up-to-date. 2. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	NIST 800-53 MA-3 NIST 800-53 MA-4 ARS MA-3.1 ARS MA-3.2 ARS MA-3.4 ARS MA-4.2 PISP 4.2.5.3 PISP 4.2.5.4
	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: 5.12.1	
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

Category: ***Service Continuity***

	General Requirement Control Technique	Protocol	Reference
5.9.11	All maintenance equipment with the capability of retaining information is checked to ensure that no sensitive information is saved on the equipment and that the equipment is appropriately sanitized prior to release. If the equipment cannot be sanitized, the equipment must remain within the facility or must be destroyed, unless an exception is specifically authorized by the SSO.	1. Review documentation supporting the contention that the required policies and procedures are up-to-date. 2. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	NIST 800-53 MA-3 ARS MA-3.3 PISP 4.2.5.3
	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: 1.3.4
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.12	Any sensitive information system being serviced is sanitized and physically disconnected from other information systems prior to allowing a remote connection, if the remote diagnostic or maintenance service organization does not have the same system level security. If the system cannot be sanitized (e.g., due to a system failure), remote maintenance is not permitted.	1. Review documentation supporting the contention that the required policies and procedures are up-to-date. 2. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	NIST 800-53 MA-4 ARS MA-4.0 PISP 4.2.5.4
	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: 1.3.4, 2.8.5
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.13	Remote diagnostic or maintenance service organizations are required to utilize the same level of security as the system being serviced. All remote maintenance sessions are audited and appropriate CMS information security personnel review the audit logs of the remote sessions. Diagnostic communications are encrypted and decrypted; strong identification and authentication techniques are used, such as tokens; and all sessions and remote connections are terminated when remote maintenance is completed. If password-based authentication is used during remote maintenance, passwords are changed following each remote maintenance service.	1. Review documentation supporting the contention that the required policies and procedures are up-to-date. 2. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	NIST 800-53 MA-4 ARS MA-4.0 ARS MA-4.1 ARS MA-4.3 PISP 4.2.5.4
	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: 2.8.5, 10.8.2
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.14	On-site repair of servers is performed within protected environments. Access to system for repair is by authorized personnel only. For off-site repair of systems, off-site access to the systems is performed by authorized personnel only. Storage media is removed before shipment for repairs. Unusable storage media is degaussed or destroyed by authorized personnel.	1. Review documentation supporting the contention that the required policies and procedures are up-to-date. 2. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.	ARS MA-CMS-2.CMS-1 ARS MA-CMS-1.CMS-1 ARS MA-CMS-2.CMS-2 PISP 4.2.5.1
	Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located.		Related CSRs: 2.2.31, 1.3.4, 5.1.4, 10.1.2
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		
5.9.15	Problems and delays encountered, including the reason and elapsed time for resolution of hardware problems, are recorded and analyzed to identify recurring patterns or trends.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of the required logs. 3. Review documentation supporting conduct of the required analyses.	FISCAM TSC-2.4.8
	Guidance: Hardware problems should be carefully analyzed in order to determine the maintenance needs and to prevent major failures.		Related CSRs:
	☑ ***SS*** ☑ ***PSC*** ☑ ***PartB*** ☑ ***PartA*** ☑ ***MAC*** ☑ ***Dmerc*** ☑ ***DC*** ☑ ***CWF*** ☑ ***COB***		

5.10 Arrangements shall be made for alternate data processing and telecommunications facilities.

5.10.1 Arrangements and agreements have been established for a backup data center and other needed facilities that: (1) are in a state of readiness commensurate with the risks of interrupted operations; (2) have sufficient processing capacity and; (3) are available for use.

1. Review documentation supporting the contention that alternate facilities have sufficient processing capacity.
2. Inspect agreements established to confirm coverage of all identified alternate facilities.
3. Review documentation identifying facilities required for alternate data processing and telecommunications.
4. Review documentation supporting the contention that alternate facilities are in the required state of readiness.
5. Review documentation supporting the contention that alternate facilities are available for use.

FISCAM TSC-3.2.1
CMS Directed
NIST 800-53 CP-7
NIST 800-53 CP-8
ARS CP-7.0
ARS CP-7.3
ARS CP-7.4
ARS CP-8.0
ARS CP-8.1
PISP 4.2.3.7
PISP 4.2.3.8

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: 2.2.28, 5.1.3, 5.4.5, 5.4.4, 5.9.7, 1.11.5

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

5.10.2 Arrangements are planned for travel and lodging of necessary disaster recovery personnel, if needed.

Verify by inspection that the required arrangements have been planned.

CMS Directed
FISCAM TSC-3.2.3

Guidance: Disaster Recovery arrangements/plans should address persons that may need to come from distant locations as well as those that are local but who may need to stay at or near the data recovery site.

Related CSRs: 5.2.5

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

5.10.3 The backup storage and alternate processing sites are configured to facilitate timely and effective recovery operations. Potential accessibility problems to the sites in the event of an area-wide disruption or disaster are identified, and explicit mitigation actions are documented.

1. Review documentation supporting the contention that alternate facilities are available for use and geographically separated.
2. Examine the alternate sites to determine if they are available and accessible.
3. Examine policies and procedures to determine if specific parties are assigned responsibilities and specific actions are defined.

NIST 800-53 CP-6
NIST 800-53 CP-7
ARS CP-6.2
ARS CP-6.3
ARS CP-7.2
PISP 4.2.3.6
PISP 4.2.3.7

Guidance: The alternate sites should be configured to allow for a timely recovery process. They should be geographically separated so as not to be susceptible to the same type of disruption or disaster.

Related CSRs: 5.4.4

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

5.10.4 Alternate telecommunication services have been arranged. Alternate telecommunication providers do not share a single point of failure with primary telecommunications services, are sufficiently separated from the primary telecommunications services to prevent susceptibility to the same hazards, and have adequate Contingency Plans.

Review documentation confirming the arrangement of alternate telecommunication services.

ARS CP-8.1
ARS CP-8.2
FISCAM TSC-3.2.2
NIST 800-53 CP-8
ARS CP-8.3
ARS CP-8.4
ARS CP-8.0
PISP 4.2.3.8

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, 1.11.5

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

5.11 A Contingency Plan shall exist for any standalone computer workstations that specifies where backup data, software, and current operating procedures are stored.

5.11.1 A Contingency Plan is available for each standalone computer workstation that specifies where backup data and software are stored. A single plan can cover more than one workstation.

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

CMS Directed

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

Related CSRs: 5.4.5, 1.13.1, 1.13.5, 2.2.19, 5.4.1

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

5.11.2 Standalone computer workstation backup data, software, and current operating procedures are stored in accordance with the Contingency Plan.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Through inspection for a sample of standalone workstations, establish that the specified storage criteria are met.

CMS Directed

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

Related CSRs: 5.2.8, 5.4.4, 5.4.5, 5.9.7

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

5.12 Detection of malicious software shall be performed.

5.12.1 The CMS Business Partner uses specialized software to accomplish identification, detection, protection, and elimination of malicious software, including viruses, spam, and spyware. The software is managed centrally and automatically updated with the latest virus definitions and protection mechanisms whenever new releases are available.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Confirm by inspection that the required software is installed and operational in accordance with documented policy.

FISCAM TCC-1.3.2
HIPAA 164.308(a)(5)(ii)(B)
NIST 800-53 SI-3
NIST 800-53 SI-8
ARS SI-3.1
ARS SI-8.1
ARS SI-8.2
PISP 4.2.6.3
PISP 4.2.6.8

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

Related CSRs: 1.1.1, 1.9.4, 2.2.24, 10.2.2, 1.13.8, 1.13.9, 5.9.10

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

5.12.2 Malicious code protection is implemented at information system entry points, including firewalls, e-mail servers, remote access servers, workstations, servers, and mobile computing devices. Automated mechanisms are employed to detect and eradicate malicious code transported by e-mail, e-mail attachments, and removable media.

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.

NIST 800-53 SI-3
ARS SI-3.0
PISP 4.2.6.3

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

Related CSRs: 1.9.4, 1.13.9, 10.2.3

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

6. *Application Software Development and Change Control*

6.1 Emergency changes to application software shall be promptly tested and approved.

6.1.1 Emergency changes are documented and approved by appropriate operations management, formally reported to appropriate computer operations management for follow-up, and approved after the fact by appropriate programming and user management.

1. Review the documented procedure required to process emergency changes.
2. Review the documentation of emergency change procedures.
3. Interview the operations supervisor, computer operations management, programming supervisors, and user management.
4. For a sample of emergency changes, observe the required documentation and approval steps.
5. Review test plans and reports for the emergency changes.

FISCAM TCC-2.2.2
FISCAM TCC-2.2.1

Guidance: Ensure that the procedures for making emergency software changes are current and that emergency software changes are subsequently tested.

Related CSRs: 6.3.9, 6.6.1, 2.4.1, 2.4.2, 1.9.3, 5.6.3

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

6.2 Use of public domain and personal software shall be restricted.

6.2.1 Clear policies restricting the use of personal and public domain software have been developed and are enforced. Business rules and technical controls enforce the documented authorizations and prohibitions. Controls also prohibit the installation of any software by individuals other than by authorized information system or security personnel, unless authorized, in writing, by the SSO.

1. Review the required policies, and verify that they are enforced.
2. Interview the security administrator..
3. Interview users.

FISCAM TCC-1.3.1
NIST 800-53 SA-7
ARS SA-7.CMS-1
PISP 4.1.3.7

Guidance: It may be necessary to periodically randomly inspect disk drives and servers to ensure that only approved personal or public domain software is resident.

Related CSRs: 1.13.2, 1.13.8

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

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.1 If new information systems are designed and implemented, the security engineering principles detailed in NIST SP 800-27 Rev. A are used. A configuration management plan that describes change control mechanisms, tracks security flaws, and defines change authorization requirements for the system is developed and implemented during system development.

1. Review documentation establishing that existing safeguards provide the required protections.
2. Review relevant policies and procedures for inclusion and directed use of the required process.

NIST 800-53 SA-8
NIST 800-53 SA-10
ARS SA-8.0
ARS SA-10
PISP 4.1.3.8
PISP 4.1.3.10

Guidance: Policies and procedures should exist that address these control objectives.

Related CSRs: 10.7.2

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

6.3.2 A system development life cycle (SDLC) methodology has been developed that: (1) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (2) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; (3) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements; (4) complies with the information security steps of IEEE 12207.0 standard for SDLC as defined by CMS and/or the CMS Framework.

1. Interview the system manager.
2. Confirm that the SDLC includes the four required elements.

FISCAM TCC-1.1.1
NIST 800-53 SA-3
ARS SA-3.CMS-1
PISP 4.1.3.3

Guidance: Ensure that a current SDLC methodology exists, addresses security has been reviewed, and is being followed.

Related CSRs: 1.12.5

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

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

	General Requirement Control Technique	Protocol	Reference
6.3.3	Security policy assigns responsibility to Application System Managers for ensuring that appropriate administrative, physical and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.	1. Interview system programmers and administrators. 2. Interview the application system managers. 3. Review the documented policy to ensure that the required responsibilities are assigned.	CMS Directed HIPAA 164.310(a)(1)

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, 1.5.5, 1.9.9, 5.7.2

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

6.3.4	Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	1. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current. 2. Examine training plans and records. 3. Interview the programming staff and the software staff.	FISCAM TCC-1.1.2

Guidance: Training plans and materials should exist for training in SDLC methodology.

Related CSRs: 6.8.1

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

6.3.5	Changes to detailed system specifications are prepared by the programmer and reviewed by the appropriate supervisor or manager.	1. Interview the programming supervisor. 2. Review documented changes to system specifications.	FISCAM TCC-2.1.2 NIST 800-53 CM-3 PISP 4.2.4.3

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: 10.7.2

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

6.3.6	Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.	1. Interview the software programming supervisor. 2. Review documented software changes to verify the tracing process.	FISCAM TCC-2.1.3

Guidance: There should be documentation that provides a logical trace from initial requirements and specifications through to finished tested code, with no gaps in the trace path.

Related CSRs: 2.11.1, 3.5.5, 6.1.1, 10.7.2, 6.7.1, 3.4.1

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

6.3.7	Test plan standards have been developed and are followed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).	1. Ensure through observation or interviews that during testing persons/groups fulfilled their responsibilities. 2. Review test plan standards, and confirm that they follow all levels of testing and responsibilities. 3. Interview department supervisors to verify their compliance with test plan standards.	FISCAM TCC-2.1.1

Guidance: A good practice is to have independent tests performed.

Related CSRs: 1.4.3, 2.5.7

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

6.3.8	Test plans are documented and approved that define responsibilities for each party involved.	1. Interview test manager, and others as deemed necessary. 2. Interview the system manager. 3. Verify that test plans are documented and approved, and define the required responsibilities.	FISCAM TCC-2.1.4

Guidance: Persons involved in testing may include system analysts, programmers, quality assurance analysts, data base managers, security analyst, network analyst, software library control staff, users, system administrators, and test planners.

Related CSRs: 2.5.7

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

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

	General Requirement Control Technique	Protocol	Reference
6.3.9	Unit, integration and system testing are performed and approved in accordance with the test plan. A sufficient range of valid and invalid conditions is applied.	1. For the software change request selected: (1) Compare test documentation with related test plans; (2) Analyze test failures to determine if they indicate ineffective software testing. 2. Review test plan to ensure that it addresses test levels and conditions.	FISCAM TCC-2.1.5

Guidance: The test plan should be carefully reviewed to ensure that all necessary levels of testing are described and that test conditions are clearly defined. Test standards should be available.

Related CSRs: 2.5.6, 2.5.7, 3.5.1

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

6.3.10	A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live test data are not to be used in testing.	1. Confirm the restrictions in the use of live data. 2. Interview test programmers. 3. Interview the system manager. 4. Verify that test data will meet all processing criteria.	FISCAM TCC-2.1.6 FISCAM TCC-2.1.7

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: 1.9.4, 2.5.6, 2.5.7, 3.5.1, 4.7.5, 5.9.4, 6.4.1, 9.8.1

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

6.3.11	Test results are reviewed and documented.	1. Verify that test results are reviewed and documented. 2. Interview the system manager.	FISCAM TCC-2.1.8

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: 2.5.6

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

6.3.12	Program changes are controlled as they progress through testing and are moved into production only upon documented approval from users and system development management.	1. Interview user management. 2. Verify the documented approval of program changes before production implementation. 3. Interview system development management.	FISCAM TCC-2.1.9

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: 3.4.1

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

6.3.13	Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented, or when system security controls are added or modified.	1. Review documentation of all required departments for prompt and accurate updating. 2. Interview the system manager. 3. Interview the document control person (librarian).	FISCAM TCC-2.1.10

Guidance: Documentation used by hardware, software, operations, and systems persons should reflect the latest system and software environment.

Related CSRs: 1.9.4, 1.8.3, 2.5.1, 2.5.6, 3.4.5, 5.4.3, 5.8.1, 6.5.2, 5.9.4, 1.9.3, 10.7.2, 3.4.3, 4.1.5

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

General Requirement Control Technique		Protocol	Reference
6.3.14	Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	1. Interview the system programmers and/or system administrator. 2. Determine when the last production program change was reviewed, and how often. 3. Interview data center management and/or the security administrator.	FISCAM TCC-2.1.11 NIST 800-53 CM-3 PISP 4.2.4.3

Guidance: Access controls and change controls should be periodically reviewed and/or tested to ensure their proper function.

Related CSRs: 3.1.2, 3.1.3, 3.3.3, 3.4.1, 4.4.1, 7.3.6

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

6.3.15	The flaw remediation process (e.g., hotfixes, patches, service packs) is managed centrally and updates (including virus definitions) are installed automatically without individual user intervention. Automated mechanisms are employed periodically to determine the state of information system components with regard to flaw remediation.	1. Review configuration management logs/procedures. 2. Review change approval policies and procedures. 3. Interview selected personnel with system and information integrity responsibilities to determine if established procedures are followed.	NIST 800-53 SI-2 ARS SI-2.0 ARS SI-2.1 ARS SI-2.2 ARS SI-3.2 NIST 800-53 SI-3 PISP 4.2.6.2 PISP 4.2.6.3

Guidance: It is important that there be expeditious installation of service packs, patches, and virus definitions while managing proper configuration management controls centrally.

Related CSRs: 1.9.4

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

6.3.16	Immediate (as required functionality allows) installation of vendor-supplied service packs, hot fixes, security patches, and virus definitions is enforced. Vendor-supplied security patches are obtained, analyzed for security and functionality in a test bed environment, and implemented on production equipment within 72 hours, or sufficient workaround procedures are implemented protect system assets.	1. Review system configuration logs. 2. Review configuration management logs/procedures. 3. Review change approval policies and procedures. 4. Determine if any security fix has not been implemented and time of availability.	NIST 800-53 MA-2 NIST 800-53 SI-2 ARS MA-2.0 ARS SI-2.0 PISP 4.2.5.2 PISP 4.2.6.2

Guidance: It is important that there be expeditious installation of service packs, patches, and virus definitions while maintaining proper controls configuration management and testing procedures.

Related CSRs: 1.9.4

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

6.4 Access to program libraries shall be restricted.

6.4.1	Separate libraries are maintained for program development and maintenance, testing, and production programs. Production source code is maintained in a separate archive library.	1. Interview library control personnel. 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. 3. Monitor libraries in use.	FISCAM TCC-3.2.1 FISCAM TCC-3.2.2

Guidance: The separate libraries should each have their own set of access controls so that, for example, testers cannot access production code. The separate archive library should be protected from unauthorized access by software or physical controls.

Related CSRs: 2.10.2, 6.8.1, 2.2.22

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

6.4.2	Access to all programs, including production code, source code, and extra program copies, is protected by access control software and operating system features.	1. For critical software production programs, determine whether access control software rules are clearly defined. 2. Determine if the access controls are implemented and working.	HIPAA 164.312(e)(1) FISCAM TCC-3.2.3 HIPAA 164.312(a)(1)

Guidance: Separate software libraries should be established and only the library control group should be allowed move programs between libraries. Programmers should only have access to the programs they are assigned.

Related CSRs: 5.2.8, 1.4.3, 1.5.5, 2.8.3, 3.3.1, 10.10.1, 2.10.2

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

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

General Requirement Control Technique	Protocol	Reference

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

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

FISCAM TCC-3.2.4

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

Related CSRs: 1.3.10, 2.2.13, 2.2.17, 2.8.3, 2.13.3

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

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

6.5.1 Standardized procedures are implemented to distribute new software for implementation.

Examine procedures for distributing new software.

FISCAM TCC-2.3.1

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

Related CSRs: 1.9.4, 2.11.1, 3.1.3, 3.4.1, 3.4.4, 10.7.1

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

6.5.2 The distribution and implementation of new or revised software is documented and reviewed. Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.

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

FISCAM TCC-2.3.2

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

Related CSRs: 1.9.9, 3.5.1, 6.3.13

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

6.6 Programs shall be automatically labeled and inventoried.

6.6.1 Library management software is used to produce audit trails/logs of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.

1. Interview personnel responsible for library control.
2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures.
3. Review software change control policies and procedures.

FISCAM TCC-3.1

Guidance: Software controls should be easily monitored and audited. Library management of software helps ensure that differing versions are not accidentally misidentified.

Related CSRs: 2.11.1, 3.5.5, 5.9.4, 6.1.1, 10.7.2, 10.10.1, 6.8.1, 3.4.1, 3.5.1, 1.3.11

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

6.7 Authorizations for software modifications shall be documented and maintained.

6.7.1 Software change request forms are used to document software modification requests and related approvals.

Examine a selection of software change or modification request forms for approvals.

FISCAM TCC-1.2.1

Guidance: The forms should be designed such that they help ensure that change requests are clearly communicated. The authorization form may be maintained as paper or softcopy format.

Related CSRs: 6.3.6

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

6.7.2 Change requests are approved by both system users and data processing staff.

1. Determine if the change requests for past changes have been approved.
2. Interview software development staff.
3. Identify recent software modifications and determine whether change request forms were used.

FISCAM TCC-1.2.2

Guidance: A good practice is to convene the change-control board to assure all appropriate personnel provide input and approval for software modifications and document the approval of the proposed changes.

Related CSRs: 3.4.1, 3.5.1

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

6.8 Movement of programs and data among libraries shall be controlled.

6.8.1 A group independent of users and programmers controls movement of programs and data among libraries.

Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.

FISCAM TCC-3.3.1

Guidance: Prior to moving software from a test to production environment, an independent review of the changes developed and tested should be made.

Related CSRs: 2.10.2, 3.4.2, 6.3.7, 6.4.3, 6.4.1, 6.6.1, 6.3.4

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

6.8.2 Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.

1. Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared.
2. Examine some of the images of stored code that has been changed.

FISCAM TCC-3.3.2

Guidance: An independent library control group should make the image comparisons.

Related CSRs: 3.4.1

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

7. *Application System Authorization Controls*

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

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

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

FISCAM TAN-1.1.2
FISCAM TAN-1.1.3

Guidance: It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents. Pre-numbered documents help/prevents missing or lost documents.

Related CSRs: 2.6.1, 2.13.1

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

7.1.2 For batch application systems, a batch control sheet is prepared for a group of source documents and includes: date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.

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

FISCAM TAN-1.1.4

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

Related CSRs: 2.10.2

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

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

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

FISCAM TAN-1.1.1

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

Related CSRs: 1.1.5

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

7.2 Master files shall be used to identify unauthorized transactions.

7.2.1 Before transactions are processed, they are verified using master files of approved vendors, employees, etc., as appropriate for the application.

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

FISCAM TAN-3.1.1

Guidance: It is a good practice to verify the transaction is applicable before any transactions are processed. For example, a procurement system requires approved vendors prior to processing of transactions.

Related CSRs: 2.10.2

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

7.2.2 Master files and program code that does the verification are protected from unauthorized modification.

1. Identify and observe the procedures employed that protect master files and program code.
2. Review the documented procedure covering the protection of master files and program code.
3. Inspect audit data confirming that the required process is consistently used.
4. Review documentation of software controls used in providing the required protection.

FISCAM TAN-3.1.2

Guidance: The organization should maintain an application protection policy regarding the protection and modification of application master files and program code. A recommendation could be to include the policy in the application change management process or part of the organization's security profile.

Related CSRs: 5.2.8, 2.6.1, 2.13.1

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

7.3 Data entry workstations shall be secured and restricted to authorized users.

7.3.1 Data entry workstations are connected to the system only during specific periods of the day, which corresponds with the business hours of the data entry personnel.

1. Inspect audit data confirming that the required process is consistently used.
2. Review documented procedure for workstation use.
3. Observe workstation use.

FISCAM TAN-2.1.5

Guidance: Review the workstation policy/guidelines.

Related CSRs: 1.13.1

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

7.3.2 Data entry workstations are located in physically secure environments and monitors are positioned to eliminate viewing by unauthorized persons.

1. Review System Security Plan.
2. Observe the location of workstations and their monitors.

FISCAM TAN-2.1.1
NIST 800-53 PE-5
ARS PE-5.0
PISP 4.2.2.5

Guidance: Workstations processing or connected to systems processing sensitive data are located in physically secure areas.

Related CSRs: 2.2.19, 2.2.6

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

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

General Requirement
Control Technique | **Protocol** | **Reference**

7.3.3 Each operator is required to use a unique password and identification code before being granted access to the system.

1. Interview a sample of management and data entry personnel to confirm consistent use of the documented procedure. Confirm that there is no sharing of passwords or identification codes.
2. Review documented login procedure.
3. Observe a sample of data entry login.

FISCAM TAN-2.1.4

Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses, including the use of password and identification control.

Related CSRs: 2.9.9, 2.9.3

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

7.3.4 All transactions are logged as entered, along with the UserID of the person entering the data.

1. Observe the processing of sample transactions, to ascertain that they are being logged correctly.
2. Review the documented procedure prescribing transaction logging.

FISCAM TAN-2.1.9

Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the data entry process is correct.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 8.2.1, 4.2.2, 8.1.1

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

7.3.5 When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.

1. Inspect audit data confirming that the required process is consistently used.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Observe physical area during non-business hours.

FISCAM TAN-2.1.2

Guidance: Review the workstation policy/guidelines.

Related CSRs: 1.13.1, 2.2.19

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

7.3.6 Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.

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

FISCAM TAN-2.1.8

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: 6.3.14, 2.6.1, 2.13.1, 2.13.2, 8.2.1, 2.9.10, 4.2.2, 8.1.1

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

7.4 Users shall be limited to a set of authorized transactions.

7.4.1 Authorization profiles for users or workstations limit what transactions personnel can enter.

1. Review audit controls used to assure continued application of the required procedure.
2. 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.
3. Review documented procedure for data entry to confirm enforcement of the required limitation.

FISCAM TAN-2.2.1
FISCAM TAN-2.2.2

Guidance: The supervisors should address access limitations in the ACL. Review the application processing policy/guidelines.

Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4, 10.8.4

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

7.5 Exceptions shall be reported to management for review and approval.

7.5.1 Exceptions, based on parameters established by management, are reported for their review and approval.	1. Inspect audit data confirming that the required process is consistently used. 2. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.	FISCAM TAN-3.2.1

Guidance: An exception report lists items requiring review and approval. These items may be valid, but exceed parameters established by management. For, example, in a disbursement system, all disbursements exceeding $20,000 could be reported to management for their review and approval before the disbursements are released.

Related CSRs: 1.13.1

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

7.6 Independent reviews of data shall occur before entering the application system.

7.6.1 Procedures are implemented for a multilevel review of CMS sensitive input data before it is released for processing.	1. Review documented procedure for pre-processing of data. 2. Interview a sample of supervisors and control unit personnel to confirm use of the process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAN-1.2.3 NIST 800-53 SI-10 ARS SI-10.CMS-1 PISP 4.2.6.10

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: 4.2.1

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

7.6.2 Data control unit personnel verify that source documents are properly prepared and authorized, and monitor data entry and processing of source documents.	1. Observe data entry and processing procedures. 2. Inspect audit data confirming that the required process is consistently used. 3. Interview management and data control unit personnel to confirm use of the process. 4. Review relevant policies and procedures for inclusion and directed use of the required process. 5. Observe data control unit personnel performing the verification process.	FISCAM TAN-1.2.1 FISCAM TAN-1.2.2

Guidance: The data control unit is the quality assurance personnel group that validates the data on the source documents before the data is entered. Additionally, this group can monitor the data entry process for accuracy.

Related CSRs: 8.4.5, 8.5.1, 8.5.2

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

8. *Application System Completeness Controls*

8.1 Computer sequence-checking shall be implemented.

Control Technique	Protocol	Reference
8.1.1 Sequence checking is used to identify missing or duplicate transactions. Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	1. Review reports of missing or duplicate transactions. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.2.3 FISCAM TCP-1.2.4

Guidance: The possibility of alterations, missing transactions or duplicate transactions can occur if sequence numbers are not properly processed. If a sequence number is missing it may have been deleted or misplaced. The missing or duplicate data files should be investigated and corrective actions taken. An alteration to the data files should be investigated and needed corrective actions taken. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation so that timely action(s) can be taken.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 8.2.1, 4.2.2, 7.3.4, 7.3.6, 9.6.5

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

Control Technique	Protocol	Reference
8.1.2 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.2.1

Guidance: Serial numbers for source documents assist in the tracking of source documents. Additionally, the sequence of the serial numbers processed shows that a source document has not been inadvertently missed or an unauthorized transaction has been inserted into the process.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 4.2.2

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

Control Technique	Protocol	Reference
8.1.3 Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.	1. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers. 2. Review the documented procedure that prescribes the assigning of unique sequence numbers. 3. Inspect audit data confirming that the required process is consistently used. 4. Verify, though documentation review, that the application contains automatic routines for checking sequence numbers and appropriate reports/alerts are generated when serial numbers are not processed in sequence or duplicated. 5. Interview the system owner and determine what policies and corrective action are in place when a sequence number error occurs.	FISCAM TCP-1.2.2

Guidance: This is a function of the processing application. The application developer or vendor should verify the existence of transaction serial numbers being assigned, and sequence number checking routines or modules included in the application.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 4.2.2

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

8.2 Computer matching of transaction data shall be implemented.

8.2.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.

1. Verify the application has an assigned system owner.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Inspect audit data confirming that the required process is consistently used.
4. Verify the application has the ability to insert the preassigned source document numbers matched with the associated data.

FISCAM TCP-1.3.2

Guidance: The possibility of an alteration to the data files should be investigated and needed corrective actions taken. For example, within the policy guidelines, actions should include notifying the resource owner of the violation.

Related CSRs: 7.3.4, 7.3.6, 8.1.1, 2.6.1, 2.13.1, 2.13.2, 3.1.1, 9.6.5

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

8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.

1. Verify that a system owner has been designated and when errors occur, that person is notified.
2. Review the program specifications that describe the computer matching process.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM TCP-1.3.1

Guidance: The purpose of this CSR is to ensure that data input was completed thoroughly and nothing was duplicated or left out. The possibility of an alteration to the data files should be investigated and needed corrective actions taken. For example, within the policy guidelines, actions should include notifying the resource owner of the violation.

Related CSRs: 2.6.1, 2.13.1, 2.13.2, 3.1.1, 9.3.4, 9.3.5, 4.2.2

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

8.2.3 For high-value, low-volume items, individual transactions or source documents are compared with a detailed listing of items processed by the computer.

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

FISCAM TCP-1.4

Guidance: This process is application dependent, but should be automated as much as possible. If an automated function is not available for the software, then consideration for developing such a process would improve the security of the application. High value items need special attention.

Related CSRs: 2.1.5, 2.1.7, 2.1.11

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

8.3 Reconciliations shall show the completeness of the data processed for the total cycle.

8.3.1 Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.

1. Inspect audit data confirming that the required process is consistently used.
2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.
3. Review the documented procedure describing the reconciliation process.

FISCAM TCP-2.2

Guidance: This process is application dependent, but should be automated as much as possible.

Related CSRs: 2.1.5, 2.1.7, 2.1.11

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

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

General Requirement Control Technique	Protocol	Reference
8.4 Reconciliations shall show the completeness of data processed at points in the processing cycle.		
8.4.1 Record counts and control totals are established over time and entered with transaction data, and subsequently reconciled to determine the completeness of data entry.	1. Review the documented procedures for the data entry process. 2. Review a sample of data control reports for completeness of data entry. 3. This process is application dependent, but should be automated as much as possible. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application.	FISCAM TCP-2.1.1 NIST 800-53 SI-10 ARS SI-10.CMS-1 PISP 4.2.6.10

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: 2.1.5, 2.1.7, 2.1.11

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

8.4.2 Trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed.	1. Verify that the application contains routines for process checking. The checking process should be included in applicable trailer labels. 2. Interview the supervisory application programmer to determine that system controls are in place as prescribed by the application programs. 3. Inspect audit data confirming that the required process is consistently used. 4. Review the program specifications describing the reconciliation process for accurate data entry.	FISCAM TCP-2.1.2 NIST 800-53 SI-10 ARS SI-10.CMS-1 PISP 4.2.6.10

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: 2.1.5, 2.1.7, 2.1.11

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

8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	1. Review the documented procedures describing the reconciliation process for data entry. 2. Interview the supervisory application programmer to determine implementation of automatic reconciliation in completion of computer job runs. 3. Inspect audit data confirming that the required process is consistently used. 4. Verify bends and processing errors are reconciled between the completion of one job and before the start of the next job. The reconciliation process should not stop all batch processing.	FISCAM TCP-2.1.3 NIST 800-53 SI-10 ARS SI-10.CMS-1 PISP 4.2.6.10

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: 2.1.5, 2.1.7, 2.1.11

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

	General Requirement / Control Technique	Protocol	Reference
8.4.4	System interfaces require that the sending system's output control counts equal the receiving system's input counts.	1. Review the documented procedure describing the reconciliation process between systems. 2. If an automation function is not available for the software then consideration for developing such a process would improve the security of the application. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-2.1.4 NIST 800-53 SI-10 ARS SI-10.CMS-1 PISP 4.2.6.10

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: 2.1.5, 2.1.7, 2.1.11

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

	General Requirement / Control Technique	Protocol	Reference
8.4.5	A data processing control group receives and reviews control total reports and determines the completeness of processing.	1. Review the documented procedure describing the data control group's function. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-2.1.5

Guidance: Performing the comparison of control numbers is commonly referred to as balancing, and should be done automatically by the computer, although some older systems may rely on manual balancing procedures. The control numbers for the balancing at key points should be documented, such as being printed on a control totals report, and should be reviewed by the data processing control group that monitors the completeness and accuracy of processing.

Related CSRs: 2.1.5, 2.1.7, 2.1.11, 7.6.2

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

8.5 Record counts and control totals shall be implemented on an IT System.

	General Requirement / Control Technique	Protocol	Reference
8.5.1	For on-line or real time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness of data entry and processing.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedures for the data control and data entry process for inclusion of the required process.	FISCAM TCP-1.1.2 NIST 800-53 SI-10 ARS SI-10.CMS-1 HSPD-7 G(24) PISP 4.2.6.10

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: 2.1.5, 2.1.7, 2.1.11, 7.6.2

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

	General Requirement / Control Technique	Protocol	Reference
8.5.2	User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.	1. Inspect the process and documents for developing record counts and control totals to determine data entry completeness. 2. Review the documented procedures for the data control process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TCP-1.1.1 NIST 800-53 SI-10 ARS SI-10.CMS-1 PISP 4.2.6.10

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: 2.1.5, 2.1.7, 2.1.11, 7.6.2

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

9. *Application System Accuracy Controls*

9.1 Instances of erroneous data shall be reported back to the user departments for investigation and correction.

	Control Technique	Protocol	Reference
9.1.1	Error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error. Errors are corrected by the user originating the transaction.	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. Inspect audit data confirming that the required process is consistently used. 4. Review the documented error processing and correction procedures.	FISCAM TAY-3.2.1 FISCAM TAY-3.2.2

Guidance: A good approach to tracking errors and developing procedures to minimize errors would be a detailed error list for managers and supervisors to track and expand corrective actions. Error messages should clearly indicate what the error is and what corrective action is necessary.

Some systems may use error reports to communicate to the user department the rejected transactions in need of correction. More modern systems will provide user departments access to a file containing erroneous transactions. Using a computer terminal or workstation, users can initiate corrective actions. The user responsible for originating the transaction should be responsible for correcting the error.

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.4, 4.1.1, 9.3.1, 9.3.5, 9.7.1, 9.3.2, 9.6.5

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

	Control Technique	Protocol	Reference
9.1.2	All corrections are reviewed and approved by supervisors before the corrections are reentered. (Based on the Medicare operating environment, Business Partners may have other compensating controls in place.)	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented error correction procedure for inclusion of the required process. 3. Interview a sample of supervisors and subordinate personnel to confirm use of the required process.	FISCAM TAY-3.2.3

Guidance: As part of the formal security program, policies should be in a procedures document with system security features for error-correction procedures included. All corrections should be reviewed and approved by supervisors before being reentered into the system, or released for processing if corrected from a computer terminal or workstation.

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11

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

9.2 Automated entry devices shall be used to increase data accuracy.

	Control Technique	Protocol	Reference
9.2.1	Effective use is made of automated entry devices to reduce the potential for data entry errors.	Review the documentation explaining how the specified objective is met.	FISCAM TAY-1.4

Guidance: The use of automated entry devices (e.g., optical or magnetic ink character readers) can reduce data error rates, as well as speed the entry process. IRS' use of preprinted labels, showing the taxpayer's name, address, and social security number is such an example. This information can be entered without keying the data, which ensures a more accurate and faster process. A good approach validating compliance would be to document the security features of the system that spells out the characteristics of the automated data entry devices so that an audit of the procedures and devices can easily be evaluated.

Related CSRs: 2.2.3

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

9.3 Rejected transactions shall be controlled with an automated error suspense file.

9.3.1 Rejected data are automatically written on an automated suspense file and held until corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error; (2) date and time the transaction was processed and the error identified; and (3) the identity of the user who originated the transaction.

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

FISCAM TAY-3.1.1

Guidance: As part of the formal security program, policies should be delineated in a procedures document with system security features for error-correction procedures included. A security audit review process should be documented and implemented.

Related CSRs: 9.1.1, 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.4, 4.1.1, 9.7.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5

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

9.3.2 A control group is responsible for controlling and monitoring rejected transactions.

1. Review the documented procedure describing the control group's responsibilities and duties.
2. Interview a sample of the control group to confirm operational responsibilities match those documented.

FISCAM TAY-3.1.3

Guidance: A good approach would be to document the security features of the system that spells out system monitoring characteristics and the reasons for transaction rejections. Corrective action procedures should be documented and evaluated as well.

Related CSRs: 9.1.1

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

9.3.3 The suspense file is purged of transactions as they are corrected. However, general controls effectively protect the suspense file from unauthorized access and modification.

1. Review the documentation describing how general controls provide the required protection of the suspense file.
2. Review the documented procedure for the error correction process to confirm inclusion of the specified process.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM TAY-3.1.4
FISCAM TAY-3.1.6

Guidance: The suspense file should be purged of the related erroneous transaction as the correction is made. Record counts and control totals for the suspense file should be adjusted accordingly. Suspense files are normally created as the result of data needing to be input into the system or a correction to data errors.
General controls should protect the suspense file from unauthorized access and modification, in order for the auditor to be able to rely on this control technique to reduce audit risk. A good approach would be to document the security features of the system, spelling out system monitoring characteristics and the action taken when policies are not followed.

Related CSRs: 2.8.4, 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 5.2.8

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

9.3.4 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.

1. Review the documented procedure for suspense file processing and transaction reconciliation.
2. Observe the suspense file process to confirm that the documented procedure is followed.
3. Inspect audit data confirming that the required process is consistently used.

FISCAM TAY-3.1.2

Guidance: Record counts and control totals should be developed automatically during processing of erroneous transactions to the suspense file and used in reconciling the transactions successfully processed. A control group should be responsible for controlling and monitoring the rejected transactions. The records count is a good management tool that assists in the administration of vital resources used to reconcile security transaction processing.

Related CSRs: 8.2.2

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

9.3.5 The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected errors.

1. Review the documented suspense file procedure for inclusion of the specified processes.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM TAY-3.1.5

Guidance: Periodically, the suspense file should be analyzed to determine the extent and type of transaction errors being made, and the age of uncorrected transactions. This analysis may indicate a need for a system change or some specific training to reduce future data errors. The suspense file is a good management tool that assists in the administration of vital resources used to reconcile transaction processing.

Related CSRs: 9.1.1, 8.2.2, 9.5.1, 9.6.7, 9.6.8, 3.1.5

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

9.4 Source documents shall be designed to minimize errors.

9.4.1 The source document is well-designed to aid the preparer and facilitate data entry. Transaction type and date field codes are preprinted on the source document.

1. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry".
2. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.

FISCAM TAY-1.1.1
FISCAM TAY-1.1.2

Guidance: A good approach is to have needed data entry information succinctly formatted to facilitate ease of data entry.

Related CSRs: 1.9.2, 9.9.1

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

9.5 Overriding or bypassing data validation and editing shall be restricted.

9.5.1 Overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

1. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM TAY-2.3.1
FISCAM TAY-2.3.2

Guidance: As part of the formal security program, policies should be delineated in a procedures document with system security features for error-correction procedures included. A security audit review process should be documented and implemented.

Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.4, 4.1.1, 9.3.1, 9.3.5, 9.7.1

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

9.6 Output production and distribution shall be controlled.

9.6.1 Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design.

1. Review the documented procedure assigning responsibility for output production and distribution.
2. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.

FISCAM TAY-4.1.1

Guidance: Security policies are distributed to all affected personnel to include system and application rules, rules to clearly delineate responsibility, and rules to describe expected behavior of all with access to the system.

Related CSRs: 1.4.3

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

9.6.2 The computer system automatically checks the output message before displaying, writing, and printing to make sure the output has not reached the wrong workstation device. A connection must be established to a specific device (workstation, printer, etc.) and verified by the system before transmitting data.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation confirming use of the required process.
3. Review documentation describing how the required control is implemented.

FISCAM TAY-4.1.6

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.

Related CSRs: 9.8.1, 9.8.2

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

Category: ***Application System Accuracy Controls***

	General Requirement Control Technique	Protocol	Reference
9.6.3	Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure describing the output process and supervisory review.	FISCAM TAY-4.1.7

Guidance: The printed reports are good management tools to assist in the tracking of completed tasks. Related CSRs: 1.5.2

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

9.6.4	The data processing control group, or some alternative, has a schedule by application that shows: (1) when outputs are completed; (2) when they need to be distributed; (3) who the recipients are; and (4) the copies needed. The group then reviews output products for general acceptability and reconciles control information to determine completeness of processing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the required schedule to confirm inclusion of the required elements. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM TAY-4.1.2

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted. The data control group becomes the baseline for that standard by which the output quality is measured. Related CSRs: 1.5.2, 1.5.4

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

9.6.5	Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message. They are also labeled (marked) externally with the appropriate security level classification and any distribution limitations or handling caveats of the information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review sample printed reports to verify that it contains the elements required in the Control Technique.	FISCAM TAY-4.1.3 NIST 800-53 AC-15 NIST 800-53 MP-3 ARS AC-15 ARS MP-3.0 PISP 4.3.2.15 PISP 4.2.7.3

Guidance: The printed report name, time, and date are good management tools to assist in the tracking of completed tasks. Related CSRs: 8.1.1, 8.2.1, 9.1.1, 9.7.1

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

9.6.6	Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review logs and check sample output, to verify that the required information is recorded.	FISCAM TAY-4.1.4 NIST 800-53 AC-15 ARS AC-15 PISP 4.3.2.15

Guidance: The output report log is a good management tool to assist in the tracking of completed tasks. Related CSRs: 1.5.2, 3.2.3

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

9.6.7	A control log of output product errors is maintained, including the corrective actions taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review the control log and confirm that it contains the required information.	FISCAM TAY-4.1.8

Guidance: The control log, with the suspense file, provides statistics on corrective action required and actions taken. This assists management in the status and use of its personnel and equipment resource tracking. Additionally, product errors may effect the implementation of a change request with appropriate security issues that can be addressed. Related CSRs: 2.1.1, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.4, 4.1.1, 9.3.1, 9.3.5, 9.7.1

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

9.6.8 Output from reruns is subjected to the same quality review as the original output.

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

FISCAM TAY-4.1.9

Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.

Related CSRs: 2.1.2, 2.1.2, 2.1.5, 2.1.6, 2.1.7, 2.1.11, 4.1.4, 4.1.1, 9.3.1, 9.3.5, 9.7.1

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

9.7 Reports showing the results of processing shall be reviewed by users.

9.7.1 Users review output reports for data accuracy, validity, and completeness. The reports include error reports, transaction reports, master record change reports, exception reports, and control totals balance reports.

1. Review the documented procedure describing the review process and detailed report constituency.
2. Inspect audit data confirming that the required process is consistently used.
3. Review sample reports to confirm that they include the required elements specified in the Control Technique.

FISCAM TAY-4.2

Guidance: The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness.

Related CSRs: 9.1.1, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.4.1, 3.1.5, 9.6.5

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

9.8 Programmed validation and edit checks shall identify erroneous data.

9.8.1 The following are protected from unauthorized modifications: (1) program code for data validation and editing and associated tables or files; (2) program code and criteria for test of critical calculations; and (3) exception criteria and the related program code. Programs perform limit and reasonableness checks on critical calculations.

1. Review the documented procedure describing the protection provided program code, files, or tables.
2. Observe the actions or procedures in place that protect program code, files, or tables.

FISCAM TAY-2.1.4
FISCAM TAY-2.2.1
FISCAM TAY-2.2.2

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: 5.2.8, 9.6.2, 3.4.1

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

9.8.2 Programmed validation and edits include checks for: (1) reasonableness; (2) dependency; (3) existence; (4) mathematical accuracy; (5) range; (6) check digit; (7) document reconciliation; and (8) relationship or prior data matching.

1. Review the documented procedure describing programmed validation and edits for inclusion of the specifically required checks.
2. Inspect audit data confirming that the required process is consistently used.

FISCAM TAY-2.1.1
NIST 800-53 SI-7
ARS SI-7.0
PISP 4.2.6.7

Guidance: Programmed validation and edit checks are, for the most part, the most critical and comprehensive way to ensure that the initial recording of data into the system is accurate. For example, programmed validation and edit checks can effectively start as the data are being keyed in at a computer workstation using preformatted computer screens.

Related CSRs: 9.6.2, 3.4.1

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

9.8.3 Validation and editing are performed at the computer workstation during data entry or as early as possible in the data flow and before updating the master files. All data fields are checked for errors before rejecting a transaction.

1. Review the documented procedure describing the specified validation and editing process.
2. Inspect audit data confirming that the required process is consistently used.
3. Observe the validation and edit process.

FISCAM TAY-2.1.2
FISCAM TAY-2.1.3

Guidance: Validation of the accuracy of data assists in the integrity of the data being processed.

Related CSRs: 3.4.1

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

9.8.4 Off-the-shelf integrity mechanisms such as parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes are used to detect and protect against information tampering, errors, omissions and unauthorized changes to software; and tools are used to automatically monitor the integrity of the information system and the application it hosts.

Observe the actions or procedures in place that protect Medicare data.

NIST 800-53 SI-7
ARS SI-7.0
PISP 4.2.6.7

Guidance: Programmed integrity verification routines or checks are, for the most part, the most critical and comprehensive way to ensure the integrity of Medicare data.

Related CSRs: 1.9.1

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

9.8.5 Data integrity and validation controls are used to provide assurance that Medicare information has not been altered and the system functions as intended.

Observe the actions or procedures in place that protect Medicare data.

NIST 800-53 SI-7
ARS SI-7.CMS-1
ARS SI-7.CMS-2
PISP 4.2.6.7

Guidance: Data integrity and validation controls are, for the most part, the most critical and comprehensive way to ensure the integrity of Medicare data, and ensure the system functions as intended.

Related CSRs: 1.9.1

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

9.9 When appropriate, preformatted computer workstation screens shall be used for data entry.

9.9.1 Preformatted computer workstations screens are utilized and allow prompting for data to be entered and editing of data as it is entered.

1. Review documented procedure specifying preformatted workstation screens, and describing screen prompts.
2. Observe a sample of workstation screens as personnel are processing data.
3. Interview the system administrator to confirm that the required feature is universally available..

FISCAM TAY-1.2

Guidance: A good approach is to have needed data entry information and workstation screens succinctly formatted to facilitate ease of data entry. Standards do promote efficiency and accuracy.

Related CSRs: 9.4.1

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

10. *Network*

10.1 LAN/Computer Room Access Controls shall be in place.

10.1.1 Controls are established to protect access authorization lists to secure areas such as data centers.

1. By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center.
2. Review audit data confirming control of access lists in accordance with documented procedures.
3. Review relevant policies and procedures for inclusion and directed use of the required process.

CMS Directed

Guidance: Ensure that only personnel with a need-to-know have access to the list.

Related CSRs: 2.2.17

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

10.1.2 Physical access to enclosures housing network equipment is restricted. Access to telephone closets and information system transmission lines carrying unencrypted information is restricted only to authorized maintenance personnel. Access is granted to authorized personnel only, and access is monitored and recorded.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Select a sample of network equipment locations representative of the range of types of physical locations within each facility. For these sample equipment, confirm that access to them is restricted in accordance with the documented procedure.

CMS Directed
NIST 800-53 PE-3
NIST 800-53 PE-4
ARS PE-3.CMS-3
ARS PE-4.CMS-1
PISP 4.2.2.3
PISP 4.2.2.4

Guidance: Ensure that access to the area where the network equipment is located is controlled.

Related CSRs: 2.2.1, 5.1.4, 5.9.14

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

10.2 Network system security shall be monitored for deficiencies.

10.2.1 The information system is configured to automatically verify the correct operation of system security functions upon system startup and restart, upon command by users with appropriate access, and at least on a monthly routine basis; and to notify system administration upon detection of security anomalies. Automated mechanisms are employed to support centralized management of distributed security testing and to provide centralized notification of failed security tests.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Interview select personnel to determine if the system verifies the correct operation of stated system functions.
3. Examine the system to determine if it verifies the correct operations of security functions.

NIST 800-53 SI-6
ARS SI-6.1
ARS SI-6.2
ARS SI-6.0
PISP 4.2.6.6

Guidance: Automated mechanisms should be used to verify security functions.

Related CSRs: 4.2.3, 10.9.1

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

10.2.2 Real-time file scanning is enabled. Desktop virus scanning software is installed, real-time protection and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every 12 hours. Virus-scanning software is provided at critical entry points, such as remote-access servers.

1. Confirm by inspection that virus-scanning software is installed.
2. Review relevant policies and procedures for inclusion and directed use of the required process.
3. Review documentation identifying designated critical network entry points.

CMS Directed
NIST 800-53 SI-3
ARS SI-3.CMS-1
PISP 4.2.6.3

Guidance: A formal virus protection program should be established at the Network level.

Related CSRs: 5.12.1, 10.8.6, 1.13.8, 1.13.9

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

10.2.3 Network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed on demand, and at least once every 24 hours, to identify anomalies. Alerts are generated for review and assessment by technical staff.

1. Review network logs.
2. Interview technical staff.
3. Review IDS/Firewall logs.
4. Determine the method for alerts.

NIST 800-53 AU-6
ARS AU-6.CMS-2
ARS SI-4.CMS-2
NIST 800-53 SI-4
PISP 4.3.3.6
PISP 4.2.6.4

Guidance: Anomalies should be carefully analyzed to determine if unauthorized activity is occurring. Timely alerts are needed to initiate appropriate activities.

Related CSRs: 5.12.2

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

10.2.4 Intrusion detection software is implemented providing real-time identification of unauthorized use, misuse, and abuse of computer assets by internal network users and external hackers. IDS devices are installed at network perimeter points and host-based IDS sensors on critical servers.

1. Review alarm and alert functions of any firewalls and other network perimeter access control systems to insure they are properly enabled.
2. Review operating system, user accounting, and application software audit logging processes on all host and server systems to insure they are properly enabled.
3. Review relevant policies and procedures for inclusion of the required process.
4. Review sample of intrusion detection audit logs for servers and hosts on the internal, protected, network.

CMS Directed
NIST 800-53 SI-4
ARS SI-4.2
ARS SI-4.CMS-1
PISP 4.2.6.4

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

	General Requirement **Control Technique**	**Protocol**	**Reference**
10.2.5	The information system is protected against denial-of-service attacks as defined on the following sites or within the following documents: (1) SANS Organization (www.sans.org/dosstep); (2) SANS Organization's Roadmap to Defeating DDoS; and (3) NIST CVE List. Measures are in-place to limit the effects of information flooding types of denial-of-service attacks. The ability of users to launch denial-of-service attacks against other information systems or networks is also restricted.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 SC-5 ARS SC-5.1 ARS SC-5.0 ARS SC-5.2 PISP 4.3.4.5
	Guidance: A process should be established to check these sites on a regular basis.	Related CSRs: 10.8.8	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.6	Individual IDS devices are connected to a common IDS management network using common protocols. Automated tools are employed to integrate intrusion detection tools into access control mechanisms to enable rapid response to attacks through the re-configuration of IDS settings to support attack isolation and elimination.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Examine IDS devices to determine if they use a common protocols and network. 3. Interview selected personnel to determine if IDS devices are monitored and reacted to in accordance with policies and procedures.	NIST 800-53 SI-4 ARS SI-4.1 ARS SI-4.3 PISP 4.2.6.4
	Guidance: Automated tools should be employed to integrate intrusion detection tools that allow for rapid response to attacks.	Related CSRs: 2.6.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.7	Stateful inspection and application firewall hardware and software are used. The operational failure of boundary protection mechanisms does not allow the unauthorized release of information outside of the information system boundary.	1. Review firewall hardware and software configurations to determine compliance. 2. Utilize firewall reporting capabilities to review log on accounting, active connections, and effectiveness of alert settings.	PISP 4.3.4.7 NIST 800-53 SC-7 ARS SC-7.CMS-3
	Guidance: Ensure that the stateful inspection capability is being properly utilized. Stateful inspection firewalls are third-generation firewalls that analyze packets at all OSI layers. Can be used to track connectionless protocols like UDP.	Related CSRs: 10.8.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.8	Logging on perimeter devices, including firewalls and routers, is enabled. Packet screening denials originating from untrusted networks, packet screening denials originating from trusted networks, proxy use denials, user account management, modification of packet filters, modification of proxy services, application errors, system shutdown and reboot, and system errors are logged.	1. Review router/firewall configuration. 2. Review router/firewall logs. 3. Determine expiration dates of appropriate logs.	PISP 4.3.3.2 PISP 4.2.6.11 PISP 4.2.6.12 NIST 800-53 AU-2 NIST 800-53 SI-11 NIST 800-53 SI-12 ARS AU-2.CMS-1 ARS SI-12.1 ARS SI-11.0
	Guidance: Ensure that logs from perimeter devices contain the required information, and that they are carefully reviewed on a frequent basis.	Related CSRs: 2.3.2, 10.8.5	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.2.9	Selected system elements at critical control points (e.g., servers) provide logs of user network and system activity. System audit logs are reviewed on demand, and at least once every 24 hours, for: (1) initialization sequences, (2) logons and errors, (3) system processes and performance, and (4) system resources utilization to determine anomalies. Alert notifications are generated for technical staff review and assessment. Automated mechanisms are employed to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.	1. Review documentation identifying devices selected to provide the specified logging function. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review alert notifications. 4. By inspection of a sample of the logs, confirm that they include network and system activity.	ARS SI-4.2 NIST 800-53 SI-4 PISP 4.3.3.6 PISP 4.2.6.4 CMS Directed NIST 800-53 AU-6 ARS AU-6.1 ARS AU-6.CMS-1
	Guidance: Ensure that logs are kept of network activity. Establish a policy to review network infrastructure (i.e., routers, servers, etc.) system audit logs for the required events.	Related CSRs: 2.6.1, 2.1.12, 1.9.7, 2.1.8, 2.1.14, 5.9.1, 5.9.2	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

10.2.10 System error messages are revealed only to authorized users (e.g., system administrators, maintenance personnel). Confidential information (e.g., account numbers, UserIDs, social security numbers, etc.) are not listed in error logs or associated administrative messages.

Protocol:

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Examine the system to determine if it provides timely user error messages without revealing confidential information.
3. Examine the system to determine if it provides error messages only to authorized personnel.

Reference:
PISP 4.2.6.11
NIST 800-53 SI-11
ARS SI-11.0

Guidance: Ensure that only authorized personnel with a need-to-know have access to system error messages and logs. Related CSRs: 2.9.14

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

10.2.11 The use of resources is limited by priority to ensure that lower-priority processes do not interfere with the performance and/or completion of higher-priority processes running on the information system.

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

Reference:
PISP 4.3.4.6
NIST 800-53 SC-6
ARS SC-6

Guidance: The system should be configured to automatically limit the use of system resources by established priorities. Related CSRs: 5.9.1

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

10.3 Facsimile and e-mail shall be controlled.

10.3.1 Telephone numbers of the facsimile machines receiving sensitive information are verified before transmitting data.

Protocol:

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Inspect logs confirming conduct of the required verification.

Reference:
IRS 1075 5.8@9.2.b
CMS Directed

Guidance: A good approach might be a policy that requires verification of the receiving facsimile machine's telephone number. Related CSRs: 2.12.2

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

10.3.2 When sending or receiving sensitive fax information, a trusted staff member attends both the sending and receiving fax machines, or the fax machine is located in a locked room with custodial coverage over outgoing and incoming transmissions.

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

Reference:
IRS 1075 5.8@9.2.a
CMS Directed

Guidance: a good approach might be a policy that states "If a locked room with custodial coverage is unavailable, trusted staff members are required to be at both the transmitting and receiving machines prior to transmittal." Related CSRs: 2.12.2

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

10.3.3 Fax procedures are implemented for sensitive information require a cover sheet that explicitly provides guidance to the recipient, which includes: (1) notification of sensitive data and need for protection, and (2) notice to unintended recipients to telephone the sender, collect if necessary, to report the disclosure and confirm destruction of the information.

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

Reference:
IRS 1075 5.8@9.2.c
CMS Directed
IRS 1075 5.8@9.2.c.2
IRS 1075 5.8@9.2.c.1

Guidance: Establish a formal procedure generating and attaching the required fax cover sheet. Related CSRs: 1.4.2

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

10.3.4 Controls exist to identify and monitor appropriate use of the e-mail system by employees (including malware detection), and to enforce e-mail authentication, security, privacy, and message integrity. Outgoing e-mail messages and attachments are encrypted.

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

Reference:
CMS Directed
ARS SI-4.4
NIST 800-53 SI-4
PISP 4.3.4
PISP 4.2.6.4
ARS SC-CMS-4.CMS-1

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Related CSRs: 1.4.5

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

Category: ***Network***

	General Requirement Control Technique	Protocol	Reference
10.3.5	Technical security measures are implemented for e-mail to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications network. If digital signatures are implemented, all outgoing e-mail messages are digitally signed and the digital signatures for received messages are verified.	Review relevant policies and procedures for inclusion and directed use of the required process.	PISP 4.3.3.10 PISP 4.3.4 NIST 800-53 AU-10 ARS AU-10 ARS SC-CMS-4.CMS-2

Guidance: Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.

Related CSRs: 2.2.24

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

10.3.6	Audit reviews include checks, to assure that system administrators and others with special system-level access privileges are prohibited from reading the e-mail messages of others unless authorized on a case-by-case basis by appropriate management officials.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the audit process for operation in accordance with the documented process.	CMS Directed

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: 2.1.11, 2.1.12

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

10.4 Cryptographic tools shall be controlled.

10.4.1	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs when no other means of protection exists.	1. Review documentation establishing that the required protection has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.3 HIPAA 164.312(e)(2)(ii) HIPAA 164.312(a)(2)(iv)

Guidance: In some cases—especially those involving telecommunications—it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs, both while these data and programs are “in” the computer system and while they are being transmitted to another computer system or stored on removable media, such as floppy disks, which may be held in a remote location.

Related CSRs: 1.9.1

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

10.4.2	If encryption is used, it must meet federal standards and controls for key generation, distribution, storage, use, destruction; and archiving must be implemented. For authentication to a cryptographic module, a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) encryption with a 128-bit key is used.	Review relevant policies and procedures for inclusion and directed use of the required process.	NIST 800-53 IA-7 ARS IA-7.1

Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management. Only a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key shall be used.

Related CSRs: 10.6.1

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

10.4.3	The use of application security mechanisms, such as SSL and SSH, is both enabled and forced. CMS-approved encryption and password authentication methods are used in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).	1. Review existing policies and procedures to ensure requirements of CSR specified. 2. Test security mechanisms on a periodic basis for proper operation. 3. Review mechanisms against risk assessment to identify changes required to existing mechanisms.	PISP 4.3.4 ARS SC-CMS-3.CMS-1 ARS SC-CMS-3.CMS-2

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Related CSRs: 10.5.1, 10.8.2, 10.6.1, 10.8.9

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

	General Requirement Control Technique	Protocol	Reference
10.4.4	If encryption is used as an access control mechanism or as authentication to a cryptographic module, it must meet FIPS-approved encryption standards (i.e., a minimum of Triple Data Encryption Algorithm (TDEA) encryption with a 128-bit key).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that documented controls are in place and operational.	ARS IA-7.0 NIST 800-53 IA-7 PISP 4.3.2.3 PISP 4.3.1.7 NIST 800-53 AC-3 ARS AC-3.CMS-2 ARS AC-3.CMS-1

Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management. Only a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key shall be used.

Related CSRs: 10.6.1

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

	General Requirement Control Technique	Protocol	Reference
10.4.5	Sensitive data being electronically transmitted outside of a secured network must be protected from source to destination using a FIPS-approved encryption standard, and data must be transmitted via secured communications. Cryptographic mechanisms are employed to ensure recognition of changes and to prevent unauthorized disclosure of information during transmission.	1. Confirm by inspection that documented controls are in place and operational. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of controls used to assure protection of electronically transmitted sensitive information. 4. Review documentation establishing approval of the protection methods utilized.	HIPAA 164.312(e)(2)(ii) IRS 1075 5.8@1.1 FISCAM TAC-3.2.E.1 HIPAA 164.312(a)(2)(iv) PISP 4.3.2.4 PISP 4.3.4.8 PISP 4.3.4.9 IRS 1075 5.8@1.3 IRS 1075 5.8@1.2 NIST 800-53 AC-4 NIST 800-53 SC-8 NIST 800-53 SC-9 ARS AC-4.CMS-2 ARS SC-8.1 ARS SC-8.CMS-1 ARS SC-9.1 ARS SC-9.CMS-1

Guidance: Ensure that a means of protecting sensitive information during transmittal has been implemented. Guided media is generally acceptable for internal transmissions within protected facilities. Encryption is typically required for transmission outside of protected facilities or through uncontrolled or public facilities or systems.

Related CSRs: 10.6.1

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

	General Requirement Control Technique	Protocol	Reference
10.4.6	Automated mechanisms with supporting procedures, or manual procedures for cryptographic key establishment and key management are employed. The mechanisms and procedures comply with CMS-approved cryptography standards.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that documented controls are in place and operational.	PISP 4.3.4.12 NIST 800-53 SC-12 ARS SC-12.CMS-1

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Related CSRs:

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

	General Requirement Control Technique	Protocol	Reference
10.4.7	Where the use of encryption is required by CMS Information Security Policy, federal law, or other relevant authority, all cryptographic operations (including key generation) are performed using FIPS 140-2 validated cryptographic modules operating in CMS-approved modes of operation.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that documented controls are in place and operational.	PISP 4.3.4.13 NIST 800-53 SC-13 ARS SC-13

Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment and NIST SP 800-57 provides guidance on cryptographic key management. Only a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key shall be used.

Related CSRs:

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

Category: ***Network***

	General Requirement Control Technique	Protocol	Reference
10.4.8	If public key certificates are used: (1) a certificate policy and certification practice statement is developed and implemented for the issuance of public key certificates; (2) the issuance of public key certificates to individuals is authorized by a supervisor or other appropriate Business Partner official; and (3) the issuance of public key certificates to individuals is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that documented controls are in place and operational.	PISP 4.3.4.16 PISP 4.3.4.17 NIST 800-53 SC-17 ARS SC-17 NIST 800-53 SC-16 ARS SC-16

Guidance: All reasonable mechanisms should be implemented, tested and reviewed against updated risk assessment, policies, and procedures updated to reflect actual requirements and practices.

Related CSRs:

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

10.5 Adequate Network password policies shall be implemented.

10.5.1	For password-based authentication, passwords are protected from disclosure and modification, and encrypted when stored and when transmitted outside the LAN/WAN.	1. Review documentation of controls used to assure that all systems remain configured to use the specified feature. 2. Review documentation explaining how this feature is implemented on each network and local computing environment. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM TAC-3.2.A.7 FISCAM TAC-3.2.E.1 PISP 4.3.1.5 NIST 800-53 IA-5 ARS IA-5.0

Guidance: Ensure that passwords are not transmitted as plain-text.

Related CSRs: 10.10.1, 10.4.3

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

10.6 Internet Security Policies shall be made available.

10.6.1	CMS Business Partner's Internet connections must be in accordance with Section 5 in the CMS Business Partners Systems Security Manual. When a determination for Internet use has been made, it shall include a FIPS-approved encryption method at a minimum of Triple Data Encryption Algorithm (TDEA) with a 128-bit key.	1. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement. 2. Review documentation describing protections to assure that the only interconnections allowed between the Internet and networks carrying sensitive information are the specified virtual private network connections. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review documentation describing the approved authentication process used to allow establishment of the virtual private network connection to a local network or other system carrying sensitive information.	CMS Directed PISP 4.3.1.7 PISP 4.3.4.7 NIST 800-53 IA-7 NIST 800-53 SC-7 ARS IA-7.0 ARS SC-7.1

Guidance: At present, the internet may not be used for CMS sensitive data.

Related CSRs: 10.4.3, 10.8.1, 10.8.5, 10.4.2, 10.4.4, 10.4.5

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

10.6.2	Clear privacy policies are posted on web sites, at major entry points to a web site, and on any web page where substantial personal information from the public is collected.	Review web pages for compliance.	ARS AC-8.CMS-4 NIST 800-53 AC-8 PISP 4.3.2.8 CMS Directed

Guidance: Privacy policy banners should be displayed on web pages where personal information is collected. The eGov Act of 2002 and OMB M03-22 guidance requires that agencies post privacy policies on public websites.

Related CSRs: 1.7.1, 1.4.6, 2.1.9

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

	General Requirement Control Technique	Protocol	Reference
10.6.3	Unless prior approval by CMS SSG is obtained in writing, persistent cookies are prohibited.	1. Review software configuration logs/procedures. 2. If not currently in place, procedures to delete cookies should be developed and personnel trained on procedures.	PISP 4.3.4 ARS SC-CMS-5.CMS-1
	Guidance: The absence of persistent cookies should be verifiable. A persistent cookie has an expiration date and is stored on your disk until that date. A persistent cookie can be used to track a user's browsing habits by identifying him whenever he returns to a site. Information about where you come from and what web pages you visit already exists in a web server's log files and could also be used to track users browsing habits, cookies just make it easier.	Related CSRs: 1.13.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.6.4	User responsibilities and expectations for Internet use are defined; and organizational sanctions for violations are developed, implemented, and enforced. Technical security controls are implemented to prevent users from accessing inappropriate Internet content.	1. Review documentation describing the approved authentication process used to allow establishment of Internet use or other system carrying sensitive information. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	PISP 4.2.1.8 NIST 800-53 PS-8
	Guidance: At present, the internet may not be used for CMS sensitive data.	Related CSRs: 10.8.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.7	Configuration Control Policy shall be documented and available.		
10.7.1	Purchased software is used in accordance with contract agreements and copyright laws. Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the software tracking system implemented to provide the specified controls. 3. Review documentation describing audit and inventory processes and tools in use to detect improper use of software.	CMS Directed PISP 4.1.3.6 NIST 800-53 SA-6 ARS SA-6
	Guidance: A formal program should be established regarding the use of purchased software.	Related CSRs: 1.13.3, 1.1.5, 6.5.1	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		
10.7.2	Change control is implemented to maintain control of changes to hardware, software, and security mechanisms. The change control mechanism documents system changes, enforces individual accountability, and provides sufficient detail to reverse or undo changes.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming use of the documented change-control mechanism. 3. Review documentation describing the change-control mechanism that is implemented to provide the specified controls. 4. For a sample of hardware, software, and security mechanism, determine by inspection that the configuration of the sample item matches the documented baseline configuration for the item. 5. Compare sampled data, such as device type, serial number, and software version, from the current configuration management baseline system description with corresponding hardware, software, and security mechanism implementation to confirm precise match.	CMS Directed PISP 4.2.4.3 PISP 4.2.4.5 NIST 800-53 CM-3 NIST 800-53 CM-5 ARS CM-5.1
	Guidance: A good approach might be to establish change control policies and procedures for all hardware, software, and security products.	Related CSRs: 5.9.4, 6.6.1, 3.4.1, 1.9.3, 6.3.13, 6.3.1, 6.3.5	
	☑ *SS* ☑ *PSC* ☑ *PartB* ☑ *PartA* ☑ *MAC* ☑ *Dmerc* ☑ *DC* ☑ *CWF* ☑ *COB*		

10.7.3 A current baseline configuration of the information system is developed, documented, and maintained. The baseline configuration is consistent with the CMS Architecture, and documents the system's: (1) purpose; (2) description; (3) technical operations; (4) technical access; (5) maintenance; and (6) personnel training requirements (including administrators and users).

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review current baseline configuration to determine if specified controls are documented.

PISP 4.2.4.2
NIST 800-53 CM-2

Guidance: The configuration of the information system is consistent with the CMS Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).

Related CSRs: 1.9.4

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

10.7.4 The baseline configuration, system component inventory, and any other system-related operations or security documentation is reviewed and, if necessary, updated at least once per year, and while planning major system changes/upgrades. Automated mechanisms are employed to maintain an up-to-date, complete, accurate, and readily available baseline configuration. The baseline configuration is updated during information system component installations.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review baseline configuration, system inventory, and other system-related documentation to determine if specified controls are documented.

PISP 4.2.4.2
NIST 800-53 CM-2
ARS CM-2.1
ARS CM-2.2
ARS CM-2.CMS-1

Guidance: The configuration of the information system is consistent with the CMS Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).

Related CSRs: 1.9.4

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

10.7.5 Automated mechanisms are employed to: (1) document proposed changes to the information system; (2) notify appropriate approval authorities; (3) identify approvals that have not been received in a timely manner; (4) inhibit change until necessary approvals are received; and (5) document completed changes to the information system.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation describing the automated mechanisms that are implemented to provide the specified controls.

PISP 4.2.4.3
NIST 800-53 CM-3
ARS CM-3.1

Guidance: Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes.

Related CSRs: 3.5.1

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

10.7.6 When changes to the system occur, the installation of information system components is recorded in the appropriate system documentation resource(s). Security impact analyses are conducted to determine the effects of system changes. As part of the security impact analyses, the system security features and audit activities associated with configuration changes to the information system are validated to ensure they still function properly.

1. Review relevant policies and procedures for inclusion and directed use of the required process.
2. Review documentation describing the change-control mechanism that is implemented to provide the specified controls..

PISP 4.2.4.4
NIST 800-53 CM-4
ARS CM-4.CMS-1

Guidance: The organization documents the installation of information system components. After the information system is changed, the organizations checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.

Related CSRs: 1.9.7, 1.12.5, 4.1.3

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

10.7.7 The integrity of critical files and directories is reviewed for unexpected and unauthorized changes at least daily. The review of file creation, changes, and deletions is automated; permission changes are monitored. Alert notifications are generated for technical staff review and assessment.

1. Review logs.
2. Interview IT personnel.

PISP 4.3.2.13
NIST 800-53 AC-13
ARS AC-13.CMS-1

Guidance: Procedures and/or an automated system for file integrity review and alert generation should be available and kept current. Files to be inspected include system code, application code, configuration and security related files.

Related CSRs: 3.6.1, 3.6.4, 3.6.5

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

	General Requirement Control Technique	Protocol	Reference
10.7.8	Access restrictions are enforced to limit changes to the information system. Controls are implemented and/or enabled to limit public and employee access to system-level software and administrator tools, scripts, and utilities. Automated mechanisms are employed to enforce access restrictions and to support auditing of the enforcement actions.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the access restriction mechanism that is implemented to provide the specified controls..	PISP 4.2.4.5 NIST 800-53 CM-5 ARS CM-5.1 ARS CM-5.CMS-1

Guidance: The organization documents changes to information system components. The organization audits activities associated with configuration changes to the information system.

Related CSRs: 2.1.4, 2.9.2, 3.1.3, 3.2.3

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

10.7.9	Configure the security settings of information technology products to the most restrictive mode, based upon system operational requirements. The information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the security settings mechanism that is implemented to provide the specified controls..	NIST 800-53 AC-6 PISP 4.3.2.6 PISP 4.2.4.6 NIST 800-53 CM-6 ARS CM-6.CMS-1 ARS AC-6.CMS-5

Guidance: NIST SP 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.

Related CSRs: 10.8.7, 10.8.8, 10.8.10

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

10.7.10	The use of mobile code on Medicare claims information systems or networks has been approved and the following controls are implemented: (1) usage restrictions and implementation guidance are established for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (2) the use of mobile code within the information system is documented, monitored, and controlled.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the mobile code restriction mechanism that is implemented to provide the specified controls..	PISP 4.3.4.17 NIST 800-53 SC-18 ARS SC-18

Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST SP 800-28 provides guidance on active content and mobile code. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at: http://iase.disa.mil/mcp/index.html.

Related CSRs:

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

10.8 Logical Network Access Controls shall be in place.

10.8.1	Any connection to the Internet, or other external networks or systems, occurs through the use of appropriate control interfaces, including, but not limited to, firewalls, routers, gateways, proxies, and encrypted tunnels.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing controls implemented to insure compliance with this requirement.	IRS 1075 5.8@6.1 CMS Directed FISCAM TAC-3.2.E.1 PISP 4.3.4.7 IRS 1075 5.8@6.3 IRS 1075 5.8@6.2 NIST 800-53 SC-7

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: 1.13.6, 10.2.7, 10.6.1, 10.6.4

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

Category: ***Network***

	General Requirement Control Technique	Protocol	Reference
10.8.2	Procedures for authentication are implemented to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; and (3) grant access to the functions of critical network devices.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of all required authentication functions.	HIPAA 164.312(d) CMS Directed PISP 4.3.2.17 PISP 4.2.5.4 NIST 800-53 AC-17 NIST 800-53 MA-4

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

Related CSRs: 2.9.8, 2.9.11, 10.10.2, 10.10.3, 10.4.3, 5.9.13, 10.10.4

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

10.8.3	The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored.	1. Review relevant policies and procedures for inclusion and directed use of the required process and specification of the warning message(s) to be used. 2. View the required warning message displayed on the opening screen seen by system users each type of server, workstation, and terminal used in the system. 3. For a sample, including each type of network device supporting the feature, view the required warning message displayed on the opening screen seen by anyone attempting to directly access the device from the network or console.	FISCAM TAC-3.2.E.2.1 PISP 4.3.2.8 NIST 800-53 AC-8 ARS AC-8.CMS-1

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: 1.4.6, 1.4.7

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

10.8.4	Workstations with dial-up access generate a unique identifier code before connection is completed.	1. Review documented dial-up procedure to confirm inclusion of the required features. 2. Observe a sample of dial-up connections involving each type of access controller.	FISCAM TAN-2.1.7

Guidance: If workstations have dial-up access, ensure that a unique ID code is generated for each dial-up session.

Related CSRs: 1.13.1, 7.4.1, 10.10.1

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

10.8.5	All servers allowing public access (e.g. public web servers, public e-mail servers, public DNS servers) are placed within a DMZ, and direct access is not allowed to the internal network. DMZ servers cannot access the internal network. DMZ packet filtering and proxy rules are used to provide protection for servers.	1. Review network diagrams for proper configuration in relation to 'CMS Internet Architecture document number CMS-CIO-STD-INT01'. 2. Review packet filtering/proxy rules.	PISP 4.3.4.2 PISP 4.3.4.7 PISP 4.3.4.14 NIST 800-53 SC-2 NIST 800-53 SC-7 NIST 800-53 SC-14 ARS SC-2.CMS-1 ARS SC-7.1 ARS SC-14.CMS-2

Guidance: The architecture and the use of rules should prohibit unauthorized access to all servers.

Related CSRs: 2.9.2, 10.2.8, 10.6.1, 2.3.2

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

10.8.6 All traffic for external communications is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Review packet screening rules.

PISP 4.3.2.4
PISP 4.2.4.7
PISP 4.3.4.7
NIST 800-53 AC-4
NIST 800-53 CM-7
NIST 800-53 SC-7
ARS AC-4.CMS-1
ARS CM-7.1
ARS SC-7.CMS-1

Guidance: The packet screening rules should apply only to specified firewalls and routers.

Related CSRs: 10.2.2

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

10.8.7 Automated mechanisms are employed centrally to apply and verify configuration settings. The information system is reviewed annually or on an incremental basis where all parts are addressed within a year, to identify and eliminate unnecessary functions, ports, protocols, and/or services.

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

PISP 4.2.4.6
PISP 4.2.4.7
NIST 800-53 CM-6
NIST 800-53 CM-7
ARS CM-6.1
ARS CM-7.1

Guidance: NIST SP 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.
Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services provided by information systems should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Related CSRs: 1.13.10, 10.7.9

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

10.8.8 The information system is specifically configured to prohibit and/or restrict the use of the functions, ports, protocols, and/or services as listed within the following documents/resource locations: (1) NIST Common Vulnerabilities and Exposures (www.cve.mitre.org/cve/); and (2) SANS List of Vulnerabilities (www.sans.org/top20/). All network protocols not explicitly required for system and application functionality are disabled.

1. Examine network configuration logs for compliance.
2. Randomly review network protocols on desktop systems.
3. Review the policy/procedure.

ARS CM-7.0
PISP 4.2.4.7
NIST 800-53 CM-7
ARS CM-7.1

Guidance: Develop and implement a way to verify that the protocols that are not required have been disabled.

Related CSRs: 2.3.1, 1.8.4, 10.2.5, 10.7.9

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

10.8.9 The information system uses either a shared secret (i.e., password) or digital certificate to identify and authenticate specific devices before establishing a connection.

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

PISP 4.3.1.3
NIST 800-53 IA-3
ARS IA-3.0

Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.

Related CSRs: 10.4.3, 10.10.2

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

10.8.10 The information system is configured to prohibit the remote activation of collaborative computing mechanisms (e.g., video and audio conferencing). The information system provides an explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone) which are authorized in writing by the CIO. Such authorized mechanisms are configured to provide a disconnection capability (either logically or physically) when not in use.

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

PISP 4.3.4.15
NIST 800-53 SC-15
ARS SC-15.1
ARS SC-15.CMS-1

Guidance: Policies and procedures should exist that address these control objectives.

Related CSRs: 10.7.9, 10.10.4

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

Category: ***Network***

General Requirement Control Technique	Protocol	Reference
10.9 Vulnerabilities to physical and cyber attacks shall be assessed.		
10.9.1 Penetration testing is performed as needed but at least annually, vulnerability scanning is performed at least quarterly, and an enterprise security posture review is conducted at least yearly. Findings and assessment results are documented and vulnerabilities are correlated to the Common Vulnerabilities and Exposures (CVE) naming convention.	1. Review the summary results of the penetration testing. 2. Interview SSO to determine findings and relevant documents.	PISP 4.1.1.5 PISP 4.1.4.2 NIST 800-53 CA-2 NIST 800-53 RA-5 ARS RA-5.CMS-1 NIST 800-42 Table 3.2

Guidance: There should be documentation available showing that the penetration testing was accomplished according to appropriate standards and procedures.

Related CSRs: 1.4.4, 1.9.4, 10.2.1

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

General Requirement Control Technique	Protocol	Reference
10.9.2 Information concerning incidents and common vulnerabilities and threats is shared with FedCIRC, NIPC, owners of interconnected systems, other appropriate organizations, and local law enforcement when necessary.	Review relevant policies and procedures for inclusion and directed use of the required process.	PISP 4.2.6.5 NIST 800-53 SI-5 ARS SI-5.1 HSPD-7 H(25)(b)

Guidance: There should be a process available for sharing security incidents and common vulnerabilities and threats with other the owners of interconnected systems, and federal and law enforcement authorities, when appropriate.

Related CSRs: 1.6.6, 1.4.4, 1.6.1, 1.6.2

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

General Requirement Control Technique	Protocol	Reference
10.10 Logical controls shall be implemented over telecommunications access.		
10.10.1 Communication software has been implemented to verify workstation identifications in order to restrict access through specific workstations: (1) verify UserIDs and passwords for access to specific applications; (2) control access through connections between systems and workstations; (3) restrict an application's use of network facilities; (4) protect sensitive data during transmission; (5) automatically disconnect at the end of a session; (6) maintain network activity logs; (7) restrict access to tables that define network options, resources, and operator profiles; (8) allow only authorized users to shut down network components; (9) monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back to preauthorized phone numbers; (10) restrict in-house access to telecommunications software; (11) control changes to telecommunications software; (12) ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage and; (13) restrict and monitor access to telecommunications hardware or facilities.	1. Review documentation confirming implementation of communications software having all of the required features. 2. Review audit data confirming continuing operation of all specified features of the required software.	FISCAM TAC-3.2.E.1

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: 6.4.2, 2.9.8, 2.9.12, 2.8.5, 3.4.1, 2.9.19, 2.9.9, 3.6.2, 10.5.1, 2.3.3, 10.8.4

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

General Requirement Control Technique	Protocol	Reference
10.10.2 Remote and wireless access sessions are enabled through VPN links, using authorized VPN client software. FIPS-approved encryption standards are used in combination with password authentication and certificate-based authentication. All methods of remote access are documented and monitored regularly, and each remote access method for the Medicare information system has been approved.	1. Review remote access policies/procedures. 2. Check that remote access is implemented and controlled.	PISP 4.3.2.17 PISP 4.3.2.18 NIST 800-53 AC-17 NIST 800-53 AC-18 ARS AC-17.2 ARS AC-17.CMS-2 ARS AC-18.1

Guidance: Remote access should be controlled and there should be evidence of that control.

Related CSRs: 3.6.3, 10.8.2, 10.8.9

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

General Requirement Control Technique	Protocol	Reference
10.10.3 Secure management protocols are enabled through VPN link(s) if connected to a network, and remote administration is used. FIPS-approved encryption standards are used in combination with password authentication or additional authentication protection (e.g., token-based, biometric).	Review remote access policies/procedures.	PISP 4.3.2.17 NIST 800-53 AC-17 ARS AC-17.CMS-1

Guidance: Remote administration should be carefully managed and controlled. Use of encryption features should be evaluated and approved by knowledgeable persons.

Related CSRs: 2.9.11, 10.8.2

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

	Control Technique	Protocol	Reference
10.10.4	Automated mechanisms are employed to facilitate the monitoring and control of remote access methods, and all remote access are controlled through a managed access control point.	Review relevant policies and procedures for inclusion and directed use of the required process.	PISP 4.3.2.17 NIST 800-53 AC-17 ARS AC-17.3 ARS AC-17.1

Guidance: Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). The organization permits remote access for privileged functions only for compelling operational needs. NIST SP 800-63 provides guidance on remote electronic authentication.

Related CSRs: 10.8.2, 10.8.10, 2.9.11

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

	Control Technique	Protocol	Reference
10.10.5	For wireless devices, service set identifier broadcasting is disabled and the following wireless access controls are implemented: (1) encryption protection is enabled; (2) access points are placed in secure areas; (3) access points are shut down when not in use (i.e., nights, weekends); (4) a firewall is implemented between the wireless network and the wired infrastructure; (5) MAC address authentication is utilized; (6) static IP addresses, not DHCP, is utilized; (7) personal firewalls are utilized on all wireless clients; (8) file sharing is disabled on all wireless clients; (9) Intrusion detection agents are deployed on the wireless side of the firewall; and (10) wireless activity is monitored and logged, and the logs are reviewed on a regular basis.	1. Perform testing to ensure encryption requirement is met. 2. Review relevant policies and procedures for inclusion and directed use of the required encryption and process.	PISP 4.3.2.18 NIST 800-53 AC-18 ARS AC-18.CMS-2 ARS AC-18.CMS-1 CMS Directed

Guidance: NIST SP 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards. Data sent via wireless devices should be protected using encryption.

Related CSRs: 1.13.8, 2.2.28

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