

---

# CMS

# Core Set of Security

# Requirements

## **Attachment A**

# Core Security Requirements

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

General Requirement	Protocol	Reference
Control Technique		
<b>1. Entitywide Security Program Planning and Management</b>		
1.1 Management and staff shall receive security training, security awareness, and have security expertise.		
1.1.1 Security training includes the following topics and the related procedures: (1) awareness training; (2) periodic security reminders; (3) user education concerning malicious software; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential).	1. Review training syllabus for inclusion of the required training. 2. Review a sample of training records to confirm completion of the required training. 3. Review documented procedure for generation of security reminders. 4. Review the training policy. 5. Interview a sample of site personnel to verify that documented training was received.	FISCAM HIPAA PDD 63
Guidance: A formal program should be established with a policy and a procedure. <span style="float: right;">Related CSRs: 5.12.1, 2.9.2</span>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		
1.1.2 Security skill needs are accurately identified and included in job descriptions.	1. Review a sample of job descriptions for identification of security skills required. 2. Evaluate the apparent relevance of the specified security skills to the job described.	FISCAM
Guidance: The SSO should work in conjunction with the HR department on job description updates. <span style="float: right;">Related CSRs: 3.3.3, 3.6.4</span>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		
1.1.3 All personnel (employees and contractors) are provided security awareness and security training prior to being allowed access to CMS sensitive information or data, and security awareness is repeated, minimally, on an annual basis.	1. Review training syllabus for inclusion of security awareness training. 2. Review policies and procedures for inclusion of the required process. 3. For a sample of personnel having access to sensitive information, review personnel records for documentation of receipt of security awareness training. 4. For a sample of personnel having access to sensitive information, review training documentation and job descriptions for apparent customization of security awareness training to job responsibilities. 5. Interview a sample of personnel having access to sensitive information to determine if they are aware of their responsibilities relating to handling of sensitive information. 6. Verify that records show training occurred prior to access to sensitive data.	CMS FISCAM HIPAA IRS 1075 PDD 63
Guidance: Security awareness and security training should inform personnel, including contractors and other users of information systems that support Medicare claims processing of: (1) the proper rules of behavior while using Medicare claims processing systems and information, and (2) their responsibilities in complying with security policies and procedures. Security awareness and security training is provided before allowing access to any sensitive information or system. Security awareness should be a continuing effort but it should be repeated, minimally, on an annual basis. <span style="float: right;">Related CSRs:</span>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		

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

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

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

General Requirement Control Technique	Protocol	Reference
1.3 Handling, storage, and destruction of sensitive information shall be formally controlled.		
1.3.1 Business Partners transmitting (FTI) from a main frame computer to another computer, need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission. (This CSR applies only to the COB contractor.)	<ol style="list-style-type: none"> <li>1. Review disclosure list for entries indicating that the documented process has been followed.</li> <li>2. Interview responsible individual(s) to confirm understanding of the required procedure.</li> <li>3. Review relevant policies and procedures for inclusion of the required logging process elements.</li> <li>4. For a sample of documents being received from the IRS, observe handling of receipt of sensitive information for compliance with established procedures.</li> </ol>	IRS 1075
Guidance: Transmission of FTI must be accompanied by appropriate records that will determine who released the information and what was released.	Related CSRs:	
<input type="checkbox"/> <i>SS</i> <input type="checkbox"/> <i>PartB</i> <input type="checkbox"/> <i>PartA</i> <input type="checkbox"/> <i>Dmerc</i> <input type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CSRF</i>		
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.	<ol style="list-style-type: none"> <li>1. Observe transmittal of sensitive information for compliance with established procedures.</li> <li>2. Review relevant policies and procedures for inclusion of the required logging process elements.</li> <li>3. Review disclosure list for entries indicating that the documented process has been followed.</li> <li>4. Interview responsible individual(s) to confirm understanding of the required procedure.</li> </ol>	HIPAA IRS 1075
Guidance: This is a key element in controlling information within HIPAA. This needs to address areas such as e-mail and other means of transmission of sensitive information.	Related CSRs: 2.12.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSRF</i>		
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.	<ol style="list-style-type: none"> <li>1. Evaluate the identified control procedures for inclusions of maintenance of records logging all shipping and receipts, and of periodic reconciliation of these records.</li> <li>2. Review documented procedures for control of sensitive data entering or leaving the facility.</li> <li>3. Evaluate the identified control procedures for inclusions of specific protections against erroneous or unauthorized transfers.</li> <li>4. Review policy for relevance.</li> </ol>	CMS HIPAA
Guidance: Control procedures should be documented and defined in a Procedures Manual. Another approach would be to provide periodic training.	Related CSRs: 2.2.25, 2.2.26	
A policy and set of procedures should exist allowing for the establishment of records regarding sensitive information.		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSRF</i>		

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

General Requirement	Protocol	Reference
Control Technique		
<p>1.3.4 A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.</p>	<ol style="list-style-type: none"> <li>1. Review the documented procedure for destruction of data.</li> <li>2. Verify that the reviewed procedure includes protections against sensitive data becoming available to unauthorized personnel.</li> </ol>	CMS
<p>Guidance: A good concept is to establish a formal program with a policy and procedures for developing and maintaining records. A record should be maintained that verifies who performed the destruction and when sensitive information was destroyed.</p>	Related CSRs: 1.3.5, 1.3.9	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.3.5 All retired, discarded, or unneeded sensitive data is disposed in a manner that prevents unauthorized persons from using it. All sensitive data is erased from storage media before releasing as work tapes or disks. Ensure the destruction of any sensitive information hard copy documents when no longer needed.</p>	<ol style="list-style-type: none"> <li>1. Review disposal procedures for inclusion of use of approved destruction methods during disposal of hard copy documents that are no longer needed.</li> <li>2. For a sample of employees, interview to determine that disposal procedures are known and being followed.</li> <li>3. Review disposal procedures for inclusion of use of approved sanitization procedures before release of any nonvolatile storage devices or media.</li> <li>4. Review disposal procedures for inclusion of protections against use of retired, discarded, or unneeded sensitive data by unauthorized persons.</li> </ol>	CMS HIPAA IRS 1075
<p>Guidance: A good approach assures policies and procedures exist for release and/or destruction of CMS sensitive information.</p>	Related CSRs: 1.3.4, 1.3.9	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.3.6 Sensitive data and CMS Business Partner records (Part A and Part B claims and benefit check records) are stored on-site. When on-site storage is not available, commercial storage facilities are used that most closely meet Federal standards for agency records centers. (Obtain Federal standards on National Archives Record Administration [36 CFR part 1228 subpart K]).</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. By inspection confirm that the specified data and records are stored on-site.</li> </ol>	CMS
<p>Guidance: When utilizing commercial storage facilities for off-site storage, ensure that any agreements in place address these Federal standards.</p>	Related CSRs:	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.3.7 Sensitive information is never disclosed during disposal unless authorized by statute. Destruction of sensitive information is witnessed by a CMS Business Partner employee. However, a Business Partner may elect to have the destruction certified by a shredding contractor in the absence of Business Partner participation.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review a sample of destruction records to confirm consistent use of the procedure.</li> </ol>	HIPAA IRS 1075
<p>Guidance: A formal program should be established with a policy and procedure. Review and update existing policy and procedures for addressing these requirements.</p>	Related CSRs:	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

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

General Requirement Control Technique	Protocol	Reference
<p>1.3.8 Before releasing files containing sensitive information to an individual or contractor not authorized to access sensitive information, care is taken to remove all such sensitive information. Procedures are in place to clear sensitive information and software from computers, memory areas, disks, and other equipment or media before they are disposed of or transferred to another use. The responsibility for clearing information is clearly assigned, and standard forms or a log is used to document that all discarded or transferred items are examined for sensitive information and this information is cleared before the items are released.</p> <p>Guidance: It is good practice to review the media destruction procedures. In many cases, standard formatting will not remove sensitive data. Additionally, a tracking or inventory system is used for the hardware but not the sensitive data residing in the electronic media. An approach to ensuring the sensitive data is cleared from the media is to test an reformat multiple times with an approved formatting technique.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data confirming consistent use of the required procedure.</li> </ol>	<p>FISCAM HIPAA IRS 1075</p>
<p>Related CSRs: 2.12.2, 2.14.1</p>		
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
<p>1.3.9 FTI is physically destroyed by authorized personnel, or returned to the originator or to the system security administrator. (This CSR applies only to the COB contractor.)</p> <p>Guidance: A formal security program should be established with a policy and procedure.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data confirming consistent use of the required procedure.</li> </ol>	<p>IRS 1075</p>
<p>Related CSRs: 1.3.4, 1.3.5</p>		
<p><input type="checkbox"/> <i>SS</i>      <input type="checkbox"/> <i>PartB</i>      <input type="checkbox"/> <i>PartA</i>      <input type="checkbox"/> <i>Dmerc</i>      <input type="checkbox"/> <i>DC</i>      <input type="checkbox"/> <i>CWF</i></p>		
<p>1.3.10 Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. When FTI information is returned to CMS, a receipt process is used. (This CSR applies only to the COB contractor.)</p> <p>Guidance: It is a good approach when returning FTI information to CMS to obtain a receipt, and provide a notification which contains when and why the information was obtained, how long and for what reason(s) it was used, and when it was returned so as to make the FTI information usage traceable.</p>	<ol style="list-style-type: none"> <li>1. Confirm by inspection that facility has latest version of IRS Publication 1075.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review audit data confirming consistent use of the required receipt process.</li> </ol>	<p>IRS 1075</p>
<p>Related CSRs:</p>		
<p><input type="checkbox"/> <i>SS</i>      <input type="checkbox"/> <i>PartB</i>      <input type="checkbox"/> <i>PartA</i>      <input type="checkbox"/> <i>Dmerc</i>      <input type="checkbox"/> <i>DC</i>      <input type="checkbox"/> <i>CWF</i></p>		
<p>1.3.11 Destruction methods for sensitive information are as follows: (1) burning - the material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (2) mulching or pulping - all material is reduced to particles one inch or smaller; (3) shredding or disintegrating - paper is shredded in cross-cut shredders to a residue particle size not to exceed 1/32 inch in width (with a 1/64 inch tolerance) by 1/2 inch in length, and microfilm is shredded to 1/35 inch by 3/8 inch strips.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review documentation confirming that destruction is accomplished using one or more of the approved methods.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>HIPAA IRS 1075</p>
<p>Related CSRs:</p>		
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		

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

General Requirement Control Technique	Protocol	Reference
<p>1.3.12 Inventory records of all storage media containing sensitive data must be maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media will be recorded in a log that identifies: (1) date received, (2) reel/cartridge control number contents, (3) number of records if available, (4) movement, and (5) if disposed of, the date and method of destruction. Such a log must permit all storage media containing sensitive data (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and logged.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data confirming consistent use of the required procedure.</li> </ol>	<p>CMS FISCAM HIPAA IRS 1075 PDD 63</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>1.3.13 Semiannual inventories of removable storage devices and media containing sensitive information are performed.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.</li> </ol>	<p>IRS 1075 PDD 63</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>1.3.14 Removable storage devices and media containing sensitive information are secured before, during, and after processing, and a proper acknowledgement form is signed and returned to the originator.</p> <p>Guidance: A formal program should be established with a policy and procedure.</p>	<ol style="list-style-type: none"> <li>1. Review audit data confirming consistent use of the required procedure.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>IRS 1075 PDD 63</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>1.3.15 Whenever possible computer operations are in a secure area with restricted access. Sensitive information is kept locked when not in use. Tape reels, disks, or other media are labeled as CMS Sensitive Information. Media holding, processing or storing sensitive data is kept in a secure area.</p> <p>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).</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation confirming location of computer operations are in a secure area with restricted access, or that establishes approved use of equivalent safeguards.</li> </ol>	<p>CMS HIPAA IRS 1075 PDD 63</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

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

General Requirement Control Technique	Protocol	Reference
<p>1.4 Owners and users shall be aware of security policies.</p> <p>1.4.1 Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; (6) assuring that system users, including maintenance personnel, receive security awareness training; and (7) implementing procedures to determine that the access of a workforce member to CMS sensitive information is appropriate.</p> <p>Guidance: Verify that unauthorized personnel are denied access to areas containing sensitive information.</p>	<ol style="list-style-type: none"> <li>1. Review a sample of training records to confirm completion of security awareness training.</li> <li>2. Review training syllabus for inclusion of the security awareness training.</li> <li>3. Review relevant policies and procedures for inclusion of the prescribed features.</li> <li>4. Review personnel security records and job descriptions to verify that operating and maintenance personnel have the proper clearances.</li> <li>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.</li> </ol>	HIPAA
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.4.2 To provide reasonable assurance that sensitive information is adequately safeguarded, an annual self-assessment is conducted which addresses the safeguard requirements imposed by CMS. A copy of the self-assessment is submitted to CMS.</p> <p>Guidance: Annually complete the self assessment utilizing the Contractor Assessment Security Tool (CAST), and run the "Error Check Self-Assessments."</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion of the required self assessment process.</li> <li>2. Review documentation confirming submittal of the most recent self assessment to CMS.</li> </ol>	HIPAA IRS 1075
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.4.3 Reporting Improper Inspections or Disclosures of Sensitive Information - Upon discovery by any employee, the individual making the observation or receiving the information contacts his or her supervisor, who contacts CMS for submission to the appropriate authority.</p> <p>Guidance: Establish procedures to identify apparent security violations and that suspicious activity is investigated and appropriate action taken.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies for inclusion of this directive.</li> <li>2. For a sample of employees, interview to confirm familiarity with the policy and how to report such improper activity.</li> </ol>	FISCAM HIPAA IRS 1075
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.4.4 Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; (3) rules that describe expected behavior of all with access to the system; and (4) procedures to prevent, detect, contain, and correct security violations.</p> <p>Guidance: Establish procedures to distribute the security policies to all necessary personnel, and develop a process to document the receipt by the personnel.</p>	<ol style="list-style-type: none"> <li>1. Review policies and procedures for the required distribution process(es).</li> <li>2. Review the distributed security policies for inclusion of the required rules.</li> </ol>	FISCAM HIPAA
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.4.5 Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. The procedures: (1) stipulate what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.</p> <p>Guidance: A good approach is to access the CERT WEB site for sample procedures for inclusion.</p>	<p>Review relevant policies and procedures for inclusion and directed use of the required procedures.</p>	CMS HIPAA
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

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

General Requirement	Protocol	Reference
Control Technique		
1.4.6 Medicare information is not used in the CMS Business Partner's private line of business unless authorized by CMS as consistent with the Privacy Act.	<ol style="list-style-type: none"> <li>1. Review relevant policies for inclusion of this directive.</li> <li>2. For a sample of employees, interview to confirm awareness of, and adherence to this policy.</li> </ol>	CMS
Guidance: Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.4.7 Employees are discouraged from browsing sensitive data files by making it clear that company policy prohibits it.	<ol style="list-style-type: none"> <li>1. Interview a sample of employees to confirm awareness of, and adherence to this policy.</li> <li>2. Review relevant policies for inclusion of the required directive.</li> </ol>	CMS
Guidance: Unless specifically directed by CMS, Medicare information is not to be used outside of the Medicare line of business. The employee should have a valid need-to-know.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.5 Information security responsibilities shall be clearly assigned.		
1.5.1 The system security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for: (1) information resource owners and users; (2) information resources management and data processing personnel; (3) senior management; and (4) security administrators.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>	FISCAM
Guidance: Ensure that the Rules of Behavior are contained in the SSP and that they clearly define the responsibility of all employees.	Related CSRs: 1.4.4	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.5.2 The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.	Review documentation verifying that an SSO with the required qualifications is designated at an overall level, and at any subordinate levels designated as appropriate by the Business Partner.	CMS FISCAM HIPAA
Guidance: An approach is to certify or ascertain that the SSO has a CISA, CISSP or other appropriate information security certification.	Related CSRs: 9.6.3, 9.6.5, 9.6.6	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.5.3 If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.	<ol style="list-style-type: none"> <li>1. If these additional SSO positions exist, review documentation supporting use of the specified process.</li> <li>2. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS
Guidance: Ensure that all Medicare related actions are cleared through the primary Medicare SSO.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.5.4 The SSO is organizationally independent of IS operations.	Review documentation supporting the required organizational independence.	CMS
Guidance: Ensure that the SSO's duties allow him/her to act independent of IS operations.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

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

General Requirement	Protocol	Reference
Control Technique		
<p>1.5.5 The SSO assures compliance with CMS's systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with CMS systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by CMS Regional Officer and/or Consortium; (4) ensuring that internal controls are incorporated into new ADP information systems; (5) ensuring that systems security requirements are included in RFPs and subcontracts involving Medicare claims processing; (6) maintaining systems security documentation for review by CMS Regional Officer and/or Consortium; (7) consulting with the CCMO's designated security officer on systems security issues when there is a need for guidance or interpretation; and (8) keeping up with new/advanced systems security technology; (9) is a member of all planning groups, having the responsibility to subject all new systems/installations (and major changes) to the risk assessment process; and (10) makes certain that specialists such as auditors, lawyers, and building engineers address security issues before changes are made.</p> <p>Guidance: An approach is to include these in the SSO's job description.</p>	<p>1. Review documentation supporting SSO performance of each of the specified roles and responsibilities.</p> <p>2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.</p>	<p>CMS HIPAA</p>
<p style="text-align: right;">Related CSRs: 9.6.3, 3.1.2, 1.9.4</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.5.6 The SSO in each CMS Business Partner organization is responsible for assisting Application System Managers in selecting and implementing appropriate administrative, physical, and technical safeguards for application systems under development or enhancement.</p> <p>Guidance: An approach is to include these in the SSO's job description.</p>	<p>1. Review relevant documentation for designation of this security officer.</p> <p>2. Review relevant policies and procedures for inclusion of identification of the specified roles and responsibilities of this security officer.</p>	<p>CMS</p>
<p style="text-align: right;">Related CSRs: 6.3.13</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.5.7 Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.</p> <p>Guidance: A good approach is to have the SSO designate specific employees this responsibility.</p>	<p>Review documentation supporting designation of this responsibility to specific employees.</p>	<p>FISCAM HIPAA IRS 1075</p>
<p style="text-align: right;">Related CSRs: 1.3.12</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.6 An incident response capability shall be implemented.</p>		
<p>1.6.1 Procedures exist to identify and report incidents: (1) security incident procedures; (2) report procedures; (3) response procedures; and (4) procedures to regularly review records of information system activity, such as security incident tracking reports.</p> <p>Guidance: Refer to sample procedures from the CERT WEB site.</p>	<p>1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response.</p> <p>2. Review security incident procedures</p>	<p>HIPAA</p>
<p style="text-align: right;">Related CSRs:</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.6.2 The CMS Business Partner's incident response capability has the following characteristics: (1) an understanding of the CMS Business Partners being served; (2) educated information owners and users that trust the incident handling team; (3) a means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; and (5) links to other relevant groups.</p> <p>Guidance: Refer to sample procedures from the CERT WEB site.</p>	<p>Review documentation supporting existence of the required characteristics within the Business Partner's incident response capability.</p>	<p>FISCAM</p>
<p style="text-align: right;">Related CSRs:</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		

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

**General Requirement**

<b>Control Technique</b>	<b>Protocol</b>	<b>Reference</b>
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 Partner's System Security Manual, Section 4.3.	CMS FISCAM IRS 1075
Guidance: Ensure that a policy and procedure exist to categorize and protect all Medicare sensitive data as level 3 (See BPSSM).	Related CSRs: 2.5.2, 2.7.1, 2.2.7	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		
1.8 Minimum protection standards shall consider local factors.		
1.8.1 Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.	Review relevant policies and procedures for inclusion of the required security management features.	HIPAA
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.	Related CSRs: 3.1.2, 1.9.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		
1.8.2 Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the system security plan.)	Confirm by inspection that the required documentation is on file.	FISCAM HIPAA
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.	Related CSRs: 3.1.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		
1.8.3 The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	1. Review risk assessment policy for inclusion of the required factors. 2. Review the most recent high-level risk assessment for documentation of consideration of the required factors.	FISCAM HIPAA
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.	Related CSRs: 3.1.2, 2.7.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		
1.8.4 A risk assessment is reviewed and updated annually or whenever significant modifications are made to a system, facility, or network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (policy, procedure, separating duties, security awareness and security training, testing/validating/editing, audit routines, audit trails/logs, alarms and fire extinguishing equipment, computer system automatic controls, manual controls, good housekeeping, secure disposal, authorizing/restricting access, relocating operations/equipment/records, modifying building/work environment, backup/encryption, insurance/bonding and maintenance/repair/replacement).	1. Review relevant policies and procedures for inclusion and directed use of the required process for determining the need for reassessment. 2. Review relevant policies and procedures for inclusion and directed use of the required content. 3. Review the most recent risk assessment for documented inclusion of the required content.	CMS FISCAM HIPAA PDD 63
Guidance: A good approach for this CSR is to address it as part of the formal Risk Management Program.	Related CSRs: 3.1.2, 3.1.3, 1.4.1, 2.2.19, 3.5.2, 5.9.9	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CFW</i>		

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

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

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

General Requirement	Control Technique	Protocol	Reference
1.9	A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed for each MA and GSS.		
1.9.1	The following are accomplished and documented: (1) security configuration documentation; (2) hardware/software installation and maintenance review and testing for security features; (3) inventory records; (4) security testing; and (5) checking for malicious software.	<ol style="list-style-type: none"> <li>1. Review the security plan for inclusion of the required elements.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review documentation supporting completion of the required security testing.</li> </ol>	HIPAA
	Guidance: Policies and Procedures should exist that address these 5 items.		Related CSRs: 5.9.3, 5.12.1, 2.5.1
	<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.9.2	Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.	Review relevant policies and procedures for inclusion and directed use of the required process.	HIPAA
	Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs:
	<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.9.3	A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties and covers the topics prescribed by OMB Circular A-130 such as: (a) rules of the system/application rules; (b) security awareness and security training; (c) personnel controls/personnel security; (d) incident response capability; (e) continuity of support/contingency planning; (f) technical security/technical controls; (g) system interconnection/information sharing; (h) public access controls.	<ol style="list-style-type: none"> <li>1. Review documentation verifying that a security plan covers all major facilities and operations.</li> <li>2. Review documentation verifying that the security plan has been approved by all key affected parties.</li> <li>3. Inspect the security plan to confirm that it covers all of the specified topics.</li> </ol>	FISCAM HIPAA
	Guidance: Refer to the CMS System Security Plan Methodology for further guidance.		Related CSRs: 1.8.8, 6.1.2, 6.3.4, 10.7.3
	<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.9.4	A system security plan has been prepared, in accordance with the CMS SSP Methodology, to cover every application and system categorized as a Major Application (MA) or General Support System (GSS).	<ol style="list-style-type: none"> <li>1. Review documentation establishing that preparation of the plan was in accordance with the CMS SSP Methodology.</li> <li>2. Review documentation verifying coverage by system security plans for all applications categorized as MA and GSS.</li> </ol>	CMS
	Guidance: Refer to the CMS System Security Plans Methodology for further guidance.		Related CSRs: 9.4.1, 3.2.4, 3.3.2, 3.4.6, 3.5.2, 3.5.3, 3.5.6, 3.6.2, 3.6.3, 1.8.1, 1.5.5
	<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.9.5	The CMS Business Partner System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self-assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, CMS, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10) authorization lists that include the designation of the individual responsible for handling security violations and each individual (or position title) responsible for individual assets; and (11) lists of other security records such as audit trails/logs and visitor sign-in sheets. Include all other CMS directed or Business Partners System Security Manual directed documents.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.</li> </ol>	CMS HIPAA
	Guidance: One method is to incorporate these requirements into the SSO's job description.		Related CSRs: 3.3.4, 2.2.17, 2.2.19
	<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF

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

General Requirement	Protocol	Reference
Control Technique		
1.9.6 Retention procedures are established for all CMS sensitive information.	Review documents establishing the appropriate retention procedures.	CMS HIPAA
Guidance: Review retention procedures in relation to CMS PMs.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.9.7 Documentation is available to assure that the level of sensitivity and criticality designations of each system has been assigned and has been determined to be commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.	Review documentation establishing that the required designations have been assigned with the considerations specified.	CMS
Guidance: Review the BPSSM and apply risk mitigation controls.	Related CSRs: 3.1.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.9.8 Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data verifying that vulnerability identification has been performed as specified.</li> <li>3. Establish by inspection that the required summary lists are available.</li> </ol>	PDD 63
Guidance: Review risk assessment.	Related CSRs: 1.8.9, 10.9.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.9.9 The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data supporting conduct of the required periodic reviews.</li> <li>3. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.</li> </ol>	FISCAM
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
1.9.10 The system security plan establishes a security management structure with adequate independence, authority and expertise.	<ol style="list-style-type: none"> <li>1. Verify by inspection that the system security plan contains the required management structure.</li> <li>2. Review documentation supporting the assertion that the security management structure meets the stated requirements.</li> </ol>	FISCAM
Guidance: Refer to the CMS System Security Plan Methodology for further guidance.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
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.	<ol style="list-style-type: none"> <li>1. Inspect personnel records to confirm that references have been contacted and background checks have been performed.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS FISCAM
Guidance: As part of the HR function, develop a policy and procedure to address hiring, transfer, termination, and performance items.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

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

General Requirement	Protocol	Reference
Control Technique		
<p>1.10.2 Regular job or shift rotations are required for those personnel using sensitive information.</p> <p>Guidance: Personnel whose duties or position gives them access to input or modify sensitive data in such a manner that fraud may be committed should be periodically rotated into different jobs or different shift rotations to introduce other personnel into the process. These rotations increase the likelihood that collaborative fraudulent activities by multiple employees will be disrupted and identified.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review staff assignment records to confirm that job and shift rotations occur.</li> </ol> <p>Related CSRs:</p>	FISCAM
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.10.3 Regularly scheduled vacations exceeding several days are required for those personnel using sensitive information.</p> <p>Guidance: An approach is a policy developed that requires employees using sensitive information to take a minimum of 24 hrs continuous vacation.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of personnel records to confirm compliance with the required vacation policy.</li> </ol> <p>Related CSRs:</p>	FISCAM
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.10.4 Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.</p> <p>Guidance: These items need to be addressed as part of a HR Termination/Transfer procedure.</p>	<ol style="list-style-type: none"> <li>1. Review termination and transfer procedures for inclusion of the required processes.</li> <li>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.</li> <li>3. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.</li> </ol> <p>Related CSRs: 2.9.9, 2.2.20, 2.8.1</p>	FISCAM HIPAA
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.10.5 Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.</p> <p>Guidance: CMS will provide future direction.</p>	<ol style="list-style-type: none"> <li>1. Review documentation establishing that reinvestigation policies for each position are consistent with the specified criteria.</li> <li>2. Inspect personnel records to confirm sensitive position have had background reinvestigations performed within the required period.</li> </ol> <p>Related CSRs: 2.5.5</p>	FISCAM
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>1.10.6 Confidentiality or security agreements are required for CMS Business Partner Medicare employees and their contractors assigned to work with sensitive information.</p> <p>Guidance: One method would be to include the agreements as part of the procedural policy and include a standard contract clause for all procurements.</p>	<ol style="list-style-type: none"> <li>1. Review policies on confidentiality or security agreements.</li> <li>2. Determine whether confidentiality or security agreements are on file.</li> <li>3. Review a sampling of agreements.</li> </ol> <p>Related CSRs:</p>	FISCAM HIPAA
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

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

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.	<ol style="list-style-type: none"> <li>1. Review Authorized Disclosure Agreements.</li> <li>2. Review relevant policies for inclusion and directed use of the required directive.</li> </ol>	CMS IRS 1075
Guidance: The HIPAA privacy rules should be reviewed. <span style="float: right;">Related CSRs:</span> <div style="display: flex; justify-content: space-around; align-items: center;"> <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i> </div>		
1.11.2 Written contracts or other arrangements require the inclusion of the CMS Core Security Requirements to protect the integrity, confidentiality, and availability of the electronically exchanged data. The CMS Business Partner will maintain a list of all contracts or other arrangements with other CMS Business Partners or business associates (include organization name and location, contract or agreement number, and purpose). The list of contracts will be provided to CMS in an MS Word document with the annual CAST submission.	<ol style="list-style-type: none"> <li>1. Review documented arrangements/contracts for security content.</li> <li>2. Verify risk-based decision is justified.</li> </ol>	CMS HIPAA
Guidance: A contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged should be completed prior to the exchange of data. <span style="float: right;">Related CSRs:</span> <div style="display: flex; justify-content: space-around; align-items: center;"> <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i> </div>		
1.11.3 The CMS Business Partner has obtained satisfactory assurances that all external business associates will provide appropriate safeguards for CMS sensitive information.	<ol style="list-style-type: none"> <li>1. Review the implemented safeguards.</li> <li>2. Ensure satisfactory assurances have been provided.</li> </ol>	HIPAA
Guidance: A good approach may be to provide a risk-based solution. All contracts should be part of the security profile and available to the SSO for review. <span style="float: right;">Related CSRs:</span> <div style="display: flex; justify-content: space-around; align-items: center;"> <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i> </div>		
1.12 Descriptions of Medicare operations, records, and assets are validated once a year.		
1.12.1 The System Owner/Manager, System Maintainer, or Senior Management designee signs the SSP and certification package.	Inspect the SSP and certification package for the required signatures.	CMS
Guidance: Review SSP certification package. <span style="float: right;">Related CSRs:</span> <div style="display: flex; justify-content: space-around; align-items: center;"> <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i> </div>		
1.12.2 The safeguard selection decisions and the risk assessment reports submitted are carefully reviewed.	Examine documentation supporting completion of the required review.	CMS
Guidance: Review risk assessment for mitigation of risks and provide recommendations. <span style="float: right;">Related CSRs:</span> <div style="display: flex; justify-content: space-around; align-items: center;"> <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i> </div>		
1.12.3 The CMS Business Partner is responsible for approving any necessary corrective action plans.	<ol style="list-style-type: none"> <li>1. Review audit data supporting compliance with the required approval process.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. A plan of action is documented for correcting security deficiencies.</li> </ol>	CMS
Guidance: An approach is to provide annual sign-off, by senior management, on the Corrective Action Plan. <span style="float: right;">Related CSRs: 1.8.7, 1.2.1</span> <div style="display: flex; justify-content: space-around; align-items: center;"> <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i> </div>		

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

General Requirement	Control Technique	Protocol	Reference			
1.12.4	The CMS Business Partner's systems security certification is completed annually and is fully documented.	<ol style="list-style-type: none"> <li>1. Review documentation confirming that the last CMS Business Partner's systems security certification or recertification was completed within the last year.</li> <li>2. Review documentation supporting an assertion that the security system is fully documented.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS			
	Guidance: Review SSP annual certification package(s). See the appropriate section of the BPSSM.	Related CSRs:				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.13	General workstation security requirements shall be established.					
1.13.1	Policies and procedures are implemented that specify the proper workstation functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access CMS sensitive information.	<ol style="list-style-type: none"> <li>1. Verify by inspection that the required policy/guideline is available.</li> <li>2. Interview a sample to confirm familiarity with the required document.</li> </ol>	HIPAA			
	Guidance: One approach would be to address all the local workstations as well as the workstations used at home.	Related CSRs: 7.3.3, 7.3.4, 7.3.5, 7.4.1, 7.4.2, 7.5.1				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.13.2	Policy states that employees are not permitted to bring their personally owned computers into the workplace.	Review the specified policy.	CMS			
	Guidance: Bringing personal computers into the workplace creates vulnerabilities to the Medicare resources and compromises sensitive data.	Related CSRs:				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.13.3	All CMS-owned software (such as CAST) is secured at close of business or anytime that it is not in use. Manuals and diskettes or CD-ROMs are stored out of sight in desks or file cabinets.	<ol style="list-style-type: none"> <li>1. Interview programmers and system manager.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review audit data confirming enforcement of the required process.</li> </ol>	CMS			
	Guidance: No further guidance required.	Related CSRs: 10.7.1				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.13.4	If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing the process used to assure compliance with the required policy.</li> </ol>	CMS			
	Guidance: An approach is to establish policies and procedures that address working "off-site." These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.	Related CSRs: 2.2.27				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
1.13.5	Policies are established for controlling the use of laptops, notebooks and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.	Determine the effectiveness of controlling portable terminals by review business partner mobile computing policies.	CMS			
	Guidance: An approach is to establish policies and procedures that address working "off-site." These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.	Related CSRs: 2.2.27				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF

Category: *Access Control*

General Requirement	Control Technique	Protocol	Reference
---------------------	-------------------	----------	-----------

**2. Access Control**

2.1 Audit trails/logs shall be maintained.

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

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

HIPAA

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

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

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

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

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

HIPAA  
IRS 1075

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

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

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.

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

**Category:** *Access Control*

General Requirement Control Technique	Protocol	Reference
2.1.3 All activity involving access to and modifications of sensitive or critical files is logged.	<ol style="list-style-type: none"> <li>1. Validate the types of files involved and the features are turned on or coding has been implemented.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>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.</li> <li>4. Inspect samples of the specified audit logs to confirm continuing use of the required process.</li> </ol>	FISCAM
Guidance: Access control software is used to maintain an audit trail of security accesses to determine how, when, and by whom specific actions were taken.	Related CSRs: 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.1.4 Access to audit trails/logs is restricted.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing implementation of the required restrictions.</li> <li>3. Review security software settings and compare with system security policies and procedures.</li> <li>4. Inspect a sample of audit log access lists.</li> </ol>	CMS
Guidance: Computer security managers and system administrators or managers should have read-only access for review purposes; however, security and/or administration personnel who maintain logical access functions should not have access to audit logs.	Related CSRs: 2.10.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.1.5 The audit trail includes sufficient information to establish what events occurred and who or what caused them.	<ol style="list-style-type: none"> <li>1. Review a sample of event logs and audit records to confirm the required content.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS
Guidance: In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result. Date and time can help determine if the user was a intruder or the actual person specified.	Related CSRs: 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category:** *Access Control*

<b>General Requirement</b>	<b>Control Technique</b>	<b>Protocol</b>	<b>Reference</b>			
2.1.6	Audit trails/logs are reviewed periodically (i.e., minimum of weekly) and retained for a minimum of 60 days.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of audit data confirming that audit logs are being retained for the same period as the related claim.</li> <li>3. Inspect a sample of audit data confirming that the required reviews have been conducted.</li> </ol>	CMS HIPAA			
Guidance:	Maintain, and periodically review, audit logs for critical application systems, including user-written applications. Audit logs may become evidence in legal proceedings, so care should be taken to protect their integrity	Related CSRs: 8.2.3, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 8.5.2, 9.1.1, 9.1.2, 9.1.3, 9.3.1, 9.3.3, 9.5.1, 9.6.7, 9.6.8, 3.1.5				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
2.1.7	All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.	<ol style="list-style-type: none"> <li>1. Inspect device configurations to confirm that all detected errors that can be logged are being logged.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Determine that audit logs have sufficient detail to assist with fault isolation and resolution of security abnormalities.</li> </ol>	CMS			
Guidance:	Audit trail analysis can often distinguish between operator-induced errors (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code). If a system fails or the integrity of a file (either program or data) is questioned, an analysis of the audit trail can reconstruct the series of steps taken by the system, the users, and the application. If a technical problem occurs (e.g., the corruption of a data file) audit trails can aid in the recovery process (e.g., by using the record of changes made to reconstruct the file). Correct confirmation of hardware fault routines will provide better recovery techniques and the recorded information will provide better results from hardware maintenance engineers.	Related CSRs:				
	<input type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
2.2	Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.					
2.2.1	Physical Intrusion Detection Systems (IDS) are used to provide the security of sensitive information in conjunction with other measures that provide forced entry protection during non-working hours. Alarms annunciate at an on-site protection console, a central station, or local police station. IDS include, but are not limited to: (1) door and window contacts; (2) magnetic switches; (3) motion detectors; and (4) sound detectors.	<ol style="list-style-type: none"> <li>1. Review physical intrusion detection policies and procedures for spaces and rooms containing sensitive information for inclusion of the specified approach.</li> <li>2. Review documentation describing measures used in conjunction with IDS to enhance protections provided directly by the IDS.</li> </ol>	FISCAM IRS 1075			
Guidance:	Physical security controls used to detect access to facilities and protect them from intentional and unintentional loss or impairment.	Related CSRs: 3.6.5				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

**Category: Access Control**

General Requirement	Protocol	Reference
Control Technique		
<p>2.2.2 Restricted areas are prominently posted and separated from non-restricted areas by physical barriers that control access. All entrances have controlled access (e.g., electronic access control, key access, door monitor) and the main entrance to restricted areas is manned.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing implementation of the required controls.</li> <li>3. Inspect restricted area access points to confirm that the documented controls are in place and operational.</li> </ol>	<p>CMS IRS 1075</p>
<p>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.</p>	<p>Related CSRs: 2.8.6, 5.2.7</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.2.3 All restricted areas used to protect sensitive information meet CMS criteria for secured area or security room, or provisions are made to store CMS sensitive information in appropriate security containers during non-working hours.</p>	<p>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.</p>	<p>CMS IRS 1075</p>
<p>Guidance: Review BPSSM Section 4 for guidance.</p>	<p>Related CSRs:</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.2.4 Secured areas/perimeters designed to prevent undetected entry by unauthorized persons during non-working hours are: (1) enclosed by slab-to-slab walls, constructed of approved materials, and supplemented by periodic inspection or other approved protection methods; (2) Any lesser-type partition is supplemented by UL approved electronic intrusion detection and fire detection systems; (3) Unless intrusion detection devices are used, all doors entering the space are locked and strict key or combination control is exercised. In the case of a fence and gate, the fence has intrusion detection devices or is continually guarded and the gate is either guarded or locked with intrusion alarms; and (4) The space is cleaned during working hours in the presence of a regularly assigned employee.</p>	<ol style="list-style-type: none"> <li>1. Review documentation confirming that secured area/perimeters have the required features.</li> <li>2. Inspect a sample of audit data confirming that the space is cleaned during working hours in the presence of a regularly assigned employee.</li> <li>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.</li> <li>4. Confirm by inspection that the required electronic intrusion devices are in use.</li> </ol>	<p>CMS IRS 1075</p>
<p>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.</p>	<p>Related CSRs: 2.2.5</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Access Control**

General Requirement	Protocol	Reference
Control Technique		
<p>2.2.5 Security rooms include the following features: (1) entire room is enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection; (2) all doors entering the space are locked with approved locking systems; (3) any glass in doors or walls is security glass (a minimum of two layers of 1/8-inch plate glass with .060-inch [1/32] vinyl interlayer, nominal thickness is 5/16-inch); (4) plastic glazing material is not acceptable; (5) vents and/or louvers are protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station, and is given top priority for guard/police response during any alarm situation; and (6) cleaning and maintenance is performed in the presence of an employee authorized to enter the room.</p>	<p>If Security Rooms are used, review documentation confirming that each includes all of the required features.</p>	<p>CMS IRS 1075</p>
<p>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.</p>	<p>Related CSRs: 2.2.4</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.2.6 Locking Systems for Secured Areas and Security Rooms - High-security pin-tumbler cylinder locks are used that meet the following requirements: (1) key-oriented mortised or rim-mounted deadlock bolt; (2) dead bolt throw of one inch or longer; (3) double-cylinder design; (4) cylinders have five or more pin tumblers; (5) if bolt is visible when locked, it contains hardened inserts or is made of steel; and (6) both the key and the lock are "Off Master." Convenience-type locking devices (e.g., card keys, sequence button-activated locks, etc.) used in conjunction with electric strikes are authorized for use during working hours only. Keys to secured areas are never in personal custody of an unauthorized employee and combinations are stored in a security container.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.</li> </ol>	<p>CMS IRS 1075</p>
<p>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.)</p>	<p>Related CSRs:</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.2.7 Sensitive information in any form is protected during non-working hours through a combination of a secured or locked perimeter, a secured area, or appropriate containerization.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> <li>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.</li> </ol>	<p>CMS IRS 1075</p>
<p>Guidance: Review BPSSM Section 4 for guidance.</p>	<p>Related CSRs: 1.1.8, 1.7.1</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Access Control**

General Requirement	Control Technique	Protocol	Reference
2.2.8 Sensitive information (including tapes or cartridges) are placed in secure storage in a secure location, safe from unauthorized access. All containers, rooms, buildings, and facilities containing sensitive information are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.	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.	<ol style="list-style-type: none"> <li>1. Review facility security plan for procedures and policies for protection of sensitive information.</li> <li>2. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of sensitive information data.</li> </ol>	CMS IRS 1075
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>			
2.2.9 Sensitive information outside secured areas or security rooms during non-working hours is stored in one of the following: (1) metal lateral key lock files; (2) metal lateral files equipped with lock bars on both sides and secured with security padlocks; (3) metal pull-drawer cabinets with center or off-center lock bars secured by security padlocks; or (4) key lock "mini safes" properly mounted with appropriate key control.	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.)	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements.</li> <li>3. Review documentation supporting the contention that the required process is followed for storage of sensitive information.</li> </ol>	CMS IRS 1075
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>			
2.2.10 If safes and/or vaults are used, they comply with: (1) A safe is a GSA-approved container of Class I, IV, and V, or Underwriters Laboratories (UL) listings of TRTL-30, TXTL-60, or TRTL-60; (2) A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, and uses UL-approved vault doors, and meets GSA specifications.	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.	Examine safe(s) or vault(s) for accompanying manufacturer documentation.	CMS IRS 1075
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>			
2.2.11 Locked containers must include lock mechanisms that use either a built-in key, or hasp and lock, and include the following features: (1) metal cabinet or box with riveted or welded seams, or (2) metal desks with locking drawers.	Guidance: A locked container is any metal container which is locked and to which keys and combinations are controlled.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of containers to confirm inclusion of the required features.</li> </ol>	CMS IRS 1075
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>			
2.2.12 Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.	Guidance: Workstations are located in controlled access areas and are safeguarded from unauthorized access.	Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.	HIPAA
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>			

**Category: Access Control**

General Requirement Control Technique	Protocol	Reference
2.2.13 Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Review documentation establishing the methods employed to deny access to sensitive information from unauthorized personnel during working hours.</li> </ol>	HIPAA IRS 1075
Guidance: Procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.5.1, 2.5.3		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.2.14 Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter restricted and other security areas after fire drills or other evacuation procedures.	<ol style="list-style-type: none"> <li>1. Review written emergency procedures for inclusion of the required process.</li> <li>2. Inspect a sample of audit data confirming use of the required process.</li> </ol>	FISCAM
Guidance: Re-entry access methods are used to provide appropriate controls at emergency exits. Related CSRs: 5.6.2, 2.8.8		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.2.15 Procedures exist for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges).	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of audit data confirming that the required process is consistently used.</li> </ol>	HIPAA
Guidance: Policies and procedures for limiting physical access ensure that properly authorized access is allowed. Related CSRs: 2.4.2, 2.8.9, 2.8.3		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.2.16 Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	<ol style="list-style-type: none"> <li>1. Review documentation designating specific individuals who are allowed access, and identifying the associated access control method used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review a sample of audit data confirming consistent use of the required access process.</li> </ol>	FISCAM PDD 63
Guidance: Through the use of security controls, limit access to personnel with a legitimate need for access to perform their duties. Related CSRs: 1.3.15, 2.1.2, 2.5.4, 9.2.1, 2.9.4		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Access Control**

General Requirement Control Technique	Protocol	Reference
<p>2.2.17 Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of sign-in/sign-out registers to confirm collection of the required information.</li> <li>3. Review a sample of audit data confirming compliance with the required register close out and review actions</li> <li>4. Inspect a sample of audit data confirming monthly issue of a new AAL.</li> </ol>	<p>FISCAM HIPAA IRS 1075</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CFW</i></p>		
<p>2.2.18 Management regularly reviews the list of persons with physical access to sensitive facilities.</p> <p>Guidance: Access to sensitive facilities should be limited to personnel with a legitimate need for access to perform their duties.</p>	<ol style="list-style-type: none"> <li>1. Review a sample of audit data confirming periodic completion of the required reviews.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process, and that they specify the review period.</li> </ol>	<p>FISCAM HIPAA</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CFW</i></p>		
<p>2.2.19 Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review audit data confirming consistent use of the required procedure.</li> <li>2. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.</li> </ol>	<p>FISCAM</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CFW</i></p>		
<p>2.2.20 Key combinations are changed when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.</p> <p>Guidance: There are procedures for revoking physical access to controlled areas and removing user accounts when employees terminate employment or when others, such as contractors and vendors, no longer require access.</p>	<ol style="list-style-type: none"> <li>1. Review audit data confirming consistent use of the required process.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>HIPAA IRS 1075</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CFW</i></p>		
<p>2.2.21 All entry code combinations are changed periodically.</p> <p>Guidance: Periodically changing entry codes prevents reentry by previous employees or visitors who might have knowledge of the entry code.</p>	<ol style="list-style-type: none"> <li>1. Review documentation and logs for entry code changes.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>FISCAM</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CFW</i></p>		

**Category: Access Control**

General Requirement Control Technique	Protocol	Reference
2.2.22 Unissued keys or other entry devices are secured.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.</li> </ol>	FISCAM
Guidance: Unissued keys and other entry devices should be stored in appropriate security containers. Related CSRs: <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.2.23 Keys or other access devices are needed to enter the computer room and tape/media library.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation confirming implementation and use of the required control.</li> </ol>	FISCAM HIPAA
Guidance: Access to these areas should be limited to personnel with a legitimate need for access to perform their duties. Related CSRs: 2.8.6, 10.1.1 <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.2.24 Transmission and Storage of Data - Sensitive information may only be stored on hard disk as long as the CMS Business Partner approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades and are being used. Access control devices include: (1) password security; (2) audit trails/logs; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect documentation of approval and installation of the required devices.</li> <li>3. Review documentation confirming that the access control devices include the required features.</li> <li>4. Review audit data confirming accomplishment of the required maintenance and upgrades,</li> <li>5. Review audit data confirming consistent use of the required control devices.</li> </ol>	CMS IRS 1075
Guidance: The methodology used to ensure confidentiality, both in storage and transmission, can be software based, hardware based, or a combination of both. The robustness of protection provided shall be commensurate with the sensitivity of the information. <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.2.25 Handling and Transporting Bulk Sensitive Information - Care is taken to safeguard sensitive information at all times. If hand carried between facilities, it is kept with an individual and protected from unauthorized disclosure. All shipments between facilities are documented on transmittal forms and monitored. All bulk shipments transmitted by the U.S. Postal Service, common carrier, or messenger service shall be sent in a sealed, opaque envelope, addressed by name and organization symbol, and marked "To be opened by addressee only."	<ol style="list-style-type: none"> <li>1. Review sensitive information handling and transporting policies and procedures for control technique compliance.</li> <li>2. Review sensitive information transmittal forms for accuracy and completeness.</li> <li>3. Inspect a sample of sensitive information data media for labeling compliance with the requirement.</li> </ol>	CMS
Guidance: These procedures apply for the routine and non-routine receipt, handling, and transporting of sensitive information between facilities, and are documented. However, these procedures are not meant to apply to routine claims handling and mailings between the carrier and Medicare recipients. <input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Access Control**

General Requirement		Protocol	Reference			
Control Technique						
2.2.26	Sensitive information is locked in cabinets or sealed in packing cartons while in transit. Sensitive information material remains in the custody of a CMS or CMS Business Partner employee. Accountability is maintained during the move.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of audit data supporting continuing use of the required processes.</li> </ol>	HIPAA IRS 1075			
Guidance:	The policies and procedures for protecting and transferring sensitive information materials with receipts ensure custody control and accountability during transfers.	Related CSRs: 1.3.3				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
2.2.27	Alternate work site equipment controls are: (1) only CMS Business Partner-owned computers and software are used to process, access, and store sensitive information; (2) specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with their managers or other members of the Business Partner security staff in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller, Business Partner-owned equipment is locked in a storage cabinet or desk when not in use.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process by personnel working from their homes or alternate worksites.</li> <li>2. Inspect documentation confirming that the required controls are implemented and consistently used.</li> </ol>	CMS IRS 1075			
Guidance:	Employees processing sensitive information at alternate work sites (e.g., home, other contractor or facility) must satisfy these equipment controls to properly protect sensitive information.	Related CSRs: 1.13.4, 1.13.5				
	An alternate work site is not a hotsite. Alternate work sites are those areas where employees, subcontractors, consultants, auditors, etc. perform work associated duties. The most common alternate work site is an employee's home. However, there may be other alternate work sites such as training centers, specialized work areas, processing centers, etc.					
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
2.2.28	Responsibility is assigned and security procedures are documented for bringing hardware and software into and out of the facility, as well as movement of these items within the facility, and for maintaining a record of those items.	Inspect documentation confirming that the required controls are implemented and consistently used.	HIPAA			
Guidance:	The procedures for checking all hardware and software in to and out of the facility assist in maintaining an accurate inventory.	Related CSRs:				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
2.2.29	Procedures are implemented to control access to software programs undergoing testing or revision.	Procedures are in place to protect CMS sensitive information during software testing and revisions.	HIPAA			
Guidance:	It is good practice to have an Security Test and Evaluation plan.	Related CSRs:				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
2.2.30	Policies and procedures are implemented to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).	A maintenance tracking system should be implemented.	HIPAA			
Guidance:	It is a good practice to keep an inventory of resources.	Related CSRs:				
	<input type="checkbox"/> SS	<input type="checkbox"/> PartB	<input type="checkbox"/> PartA	<input type="checkbox"/> Dmerc	<input type="checkbox"/> DC	<input type="checkbox"/> CWF
-----						
2.3	Access paths shall be identified.					
2.3.1	An analysis of the logical access paths is performed whenever changes to the system are made.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM			
Guidance:	It is important that all access paths (e.g., Internet, dial-in, telecommunications) be identified and controlled to eliminate "backdoor" paths.	Related CSRs: 3.4.1, 4.5.1				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF

**Category: Access Control**

General Requirement	Protocol	Reference
Control Technique		
2.4 Emergency and temporary access authorization shall be controlled.		
2.4.1 Procedures are established (and implemented as needed) that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	<ol style="list-style-type: none"> <li>1. Review documentation of the access control process to confirm inclusion of a procedure for emergency access.</li> <li>2. Review documentation of the access control process to confirm inclusion of at least one of the required features.</li> </ol>	HIPAA
<p>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.</p> <p style="text-align: right;">Related CSRs: 5.2.7, 5.6.2, 2.9.12</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.4.2 Emergency and temporary access authorizations are: (1) documented on standard forms and maintained on file; (2) approved by appropriate managers; (3) securely communicated to the security function and; (4) automatically terminated after a predetermined period.		
2.4.2	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect a sample of audit data confirming that all four specified elements of the required process is consistently used.</li> </ol>	FISCAM
<p>Guidance: As with normal access authorizations, emergency and temporary access should be approved and documented.</p> <p style="text-align: right;">Related CSRs: 5.2.7, 2.2.15, 2.8.3, 2.8.9</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
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.	<ol style="list-style-type: none"> <li>1. Inspect documentation identifying systems that process sensitive information.</li> <li>2. Review documentation establishing that all computers in all specified systems meet requirements in their implemented configuration.</li> <li>3. Review documentation of the configuration management process used to assure that all systems remain in certified configurations.</li> </ol>	CMS IRS 1075
<p>Guidance: The purpose of security is to support the function of the system, not to undermine it. Therefore, many aspects of the function of the system will produce related security requirements. Assurance documentation can address the security either for a system or for specific components. System-level documentation should describe the system's security requirements and how they have been implemented, including interrelationships among applications, the operating system, or networks. System-level documentation addresses more than just the operating system, the security system, and applications; it describes the system as integrated and implemented in a particular environment. Component documentation will generally be an off-the-shelf product, whereas the system designer or implementor will generally develop system documentation.</p> <p style="text-align: right;">Related CSRs: 2.2.13, 1.9.1, 2.1.2</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.5.2 Classifications and criteria have been established and communicated to resource owners.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Inspect audit data confirming that the required policy has been communicated to resource owners.</li> </ol>	FISCAM
<p>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.</p> <p style="text-align: right;">Related CSRs: 1.7.1, 2.7.1</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Access Control**

General Requirement		Protocol	Reference
Control Technique			
2.5.3	Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation establishing that existing safeguards provide the required protections.</li> </ol>	HIPAA IRS 1075 PDD 63
Guidance:	Policies and procedures limit access while ensuring that properly authorized access is allowed based on an employee's need-to-know.	Related CSRs: 2.12.1, 2.2.13, 2.7.2, 2.9.4	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
2.5.4	Sensitive information is kept separate from other information to the maximum extent possible. Files are clearly labeled to indicate that sensitive information is included. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information.	<ol style="list-style-type: none"> <li>1. Review sensitive information handling procedures for inclusion of the required processes.</li> <li>2. For a sample of media and devices containing sensitive information, inspect to confirm use of the required labels.</li> </ol>	CMS IRS 1075
Guidance:	Controlling media may require some form of physical labeling. The labels can be used to identify media with special handling instructions, to locate needed information, or to log media (e.g., with serial/control numbers or bar codes) to support accountability. Identification is often by labels on diskettes or tapes or banner pages on printouts.	Related CSRs: 2.2.16, 1.3.15, 2.2.25	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
2.5.5	Every personnel position with access to CMS sensitive information processing is designated with a sensitivity level, and documentation is available to support the security and suitability standards for these personnel commensurate with their position sensitivity level and appropriate personnel investigation requirements.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. For a sample of personnel positions, inspect documentation establishing the associated sensitivity level.</li> </ol>	CMS PDD 63
Guidance:	The staffing process generally involves: (1) defining the job, normally involving the development of a position description; (2) determining the sensitivity level of the position; (3) filling the position, which involves screening applicants and selecting an individual; and (4) security awareness training. The personnel office is normally the first point of contact in helping managers determine if a personnel investigation is necessary for a particular position. See BPSSM Section 2.	Related CSRs: 1.10.5	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
2.5.6	An independent review or audit of the security controls of all Medicare systems and applications processing sensitive information is performed at least every three years.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation verifying conduct of an independent review or audit at least every three years.</li> </ol>	FISCAM IRS 1075
Guidance:	Periodic independent assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.	Related CSRs: 1.8.6	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
2.5.7	CMS Business Partner office facilities processing sensitive information are subjected to an annual self-assessment.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	CMS FISCAM IRS 1075
Guidance:	Annual self-assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.	Related CSRs: 2.12.1, 1.4.2, 1.8.6	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>

**Category: Access Control**

<b>General Requirement</b>		<b>Protocol</b>	<b>Reference</b>
<b>Control Technique</b>			
2.5.8	Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	CMS HIPAA IRS 1075
Guidance:	Inspection, self-assessment, and corrective action reports are an important means of identifying areas of noncompliance and remedial actions performed to correct noncompliance.	Related CSRs: 1.4.2	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.5.9	Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	CMS IRS 1075
Guidance:	The procedures are used to test the security system attributes.	Related CSRs: 1.4.2, 5.7.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.5.10	Sensitive information system development documentation is available, including security mechanisms and implementation.	Inspect system design and test documentation for an explanation of security mechanisms and how they are implemented.	FISCAM
Guidance:	The system development documentation provides security mechanism and implementation review guidance to staff with varying levels of skill and experience.	Related CSRs: 6.3.7	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.5.11	Sensitive information system documentation contains the test policy, test plan, test procedures, and retest procedures, and it describes how and what mechanisms were tested, and the results.	Review the sensitive information system documentation for inclusion of required test documentation.	FISCAM
Guidance:	A disciplined process for testing and approving new and modified systems prior to their implementation is essential to ensure systems operate as intended and that no unauthorized changes are implemented. Security is an integral part of the test.	Related CSRs: 6.3.1, 6.3.9	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.6	Actual or attempted unauthorized, unusual, or sensitive access shall be monitored.		
2.6.1	Security violations and activities, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM
Guidance:	Audit functions should be activated to maintain critical audit trails and report unauthorized or unusual activity to the appropriate personnel.	Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 4.2.1, 4.2.4, 3.1.1, 10.2.3, 2.9.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Access Control**

General Requirement		Protocol	Reference
Control Technique			
2.6.2	Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.	<ol style="list-style-type: none"> <li>1. Review documentation of the controls used to enforce this requirement.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS
Guidance:	Audit trails are a mechanism that help managers maintain individual accountability. By advising computer operators that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.		
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
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.	<ol style="list-style-type: none"> <li>1. Confirm by inspection that the required procedures exist.</li> <li>2. By inspection confirm that supervisors have specified procedures.</li> </ol>	CMS
Guidance:	Procedures should be in-place to monitor visitors and contractors to insure they perform only authorized activities and work functions.		
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
-----			
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.	<ol style="list-style-type: none"> <li>1. Review resource classification documentation and compare to risk assessments.</li> <li>2. Inspect audit data confirming that the required approval and review processes are consistently used.</li> </ol>	FISCAM PDD 63
Guidance:	Resource classification determinations flow directly from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing sensitive data or failing to protect the integrity of data supporting critical transactions or decisions.		
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
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.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	CMS HIPAA IRS 1075
Guidance:	The policies and procedures for limiting access ensure that properly authorized access is allowed based on an employee's need-to-know.		
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
-----			
2.8	Resource owners shall identify authorized users and the level of authorization.		
2.8.1	Security is notified immediately when system users are terminated or transferred.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required procedure.</li> <li>2. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.</li> </ol>	FISCAM
Guidance:	Users who continue to have access to critical or sensitive resources pose a major threat, especially those who may have left under acrimonious circumstances.		
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>

**Category: Access Control**

General Requirement	Protocol	Reference
Control Technique		
<p>2.8.2 All changes to security profiles by SSO or designated representative are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming routine identification and investigation of unusual activity.</li> <li>3. Review a selection of recent profile changes and activity logs.</li> </ol>	FISCAM
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.8.3 SSOs or their designated representative review access authorizations and discuss any questionable authorizations with resource owners.</p> <p>Guidance: One method is for a listings of authorized users and their specific access needs should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security manager.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM PDD 63
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.8.4 The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. For a selection of users with dial-up access, review authorization and justification.</li> </ol>	FISCAM
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input type="checkbox"/> <i>CWF</i> </p>		
<p>2.8.5 Owners periodically review access authorization listings and determine whether they remain appropriate.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM PDD 63
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>2.8.6 Authorization lists and controls for restricted areas, such as the computer room, tape library, and workstation rooms, are maintained. Authorization lists show the following information: (1) who is authorized access to restricted areas; (2) who is authorized to operate the equipment; (3) which workstations are authorized to access the computer and computer records; and (4) who may maintain operating systems, utilities, and operational versions of application programs.</p> <p>Guidance: Authorization lists and controls for restricted areas should be part of doing business to restrict access to areas containing or processing sensitive information.</p>	<ol style="list-style-type: none"> <li>1. By inspection, confirm that authorization lists include the required information.</li> <li>2. Inspect audit data confirming continuing maintenance of authorization lists and access controls for restricted areas.</li> </ol>	CMS
<p style="text-align: right;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Access Control**

General Requirement	Protocol	Reference
Control Technique		
2.8.7 Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample representing each type of computer operating system, and for standalone and each mode of network connection affecting banner display, observe that the warning banner on the sample computer is consistent with the documented procedure.	CMS IRS 1075
Guidance: The log-on banner/screen warning banner warns the user that the system processes sensitive information and it is subject to monitoring each time they log-on.	Related CSRs: 10.8.3	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.8.8 Documented policies and procedures exist for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.	Review the appropriate documented policies and procedures for inclusion of the required rules.	HIPAA
Guidance: The policies and procedures used to grant different levels of access to sensitive information are based on an employee's need-to-know.	Related CSRs: 2.2.14	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.8.9 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to the SSO.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM
Guidance: Policies and procedures should exist for authorizing access to information resources and for documenting such authorizations.	Related CSRs: 2.14.1, 2.2.15, 1.4.1, 2.4.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.		
2.9.1 Attempts to log on with invalid passwords are limited to 3 attempts.	1. Review security software password parameters. 2. Review pertinent policies and procedures. 3. Observe the system directed action in response to four invalid access attempts, confirming that the action is consistent with the documented policy.	FISCAM
Guidance: To prevent guessing of passwords, attempts to log on the system with invalid passwords should be limited.	Related CSRs: 2.6.1, 7.3.6	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9.2 Use of names or words as passwords is prohibited.	Review relevant policies for inclusion and directed use of the required prohibition.	FISCAM
Guidance: The use of alphanumeric passwords reduces the risk that an unauthorized user could gain access to a system by using a computer to try dictionary words or names until the password is guessed.	Related CSRs: 1.1.1, 3.6.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category:** *Access Control*

<b>General Requirement</b>	<b>Protocol</b>	<b>Reference</b>
<b>Control Technique</b>		
2.9.3 Users maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others, and report lost items immediately.	<ol style="list-style-type: none"> <li>1. Interview a sample of users to confirm the required understanding and device possession.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM
Guidance: Factors that affect the use of these devices include (1) the frequency that possession by authorized users is checked, and (2) users' understanding that they should not allow others to use their identification devices.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9.4 The use of passwords and access control measures are in place to identify who accessed protected information and limit that access to persons with a need-to-know.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>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).</li> <li>3. Review documentation describing audit systems implemented to record all accesses to protected information.</li> <li>4. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description.</li> <li>5. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing.</li> <li>6. Inspect a sample of access audit data supporting continuing use to the required process.</li> </ol>	FISCAM HIPAA IRS 1075
Guidance: Logical access controls should be designed to restrict legitimate users to the specific system(s), programs, and files they need and prevent others, such as hackers, from entering the system at all.	Related CSRs: 2.7.2, 2.2.16, 2.5.3, 2.11.4, 7.4.1, 7.4.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category:** *Access Control*

General Requirement	Protocol	Reference
Control Technique		
<p>2.9.5 When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) Authentication is provided through ID and password encryption for use over public telephone lines; (2) Standard access is provided through a toll-free number and through local telephone numbers to local data facilities; and (3) Both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards should have both identification and authentication features and provides data encryption as well.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>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.)</li> <li>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.</li> <li>4. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.</li> </ol>	<p>FISCAM IRS 1075</p>
<p>Guidance: The entity should have cost-effective physical and logical controls in place for protecting systems accessed remotely. Related CSRs: 3.6.1, 3.6.3, 10.8.2</p> <p>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.</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>2.9.6 Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff after a predetermined amount of time (normally 15 minutes) and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), or (d) telephone callback procedure.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation supporting implementation of the required controls.</li> <li>3. Review a sample of audit data confirming continuing use of the required controls.</li> </ol>	<p>HIPAA</p>
<p>Guidance: Procedures should be in place to authenticate users before granting them access to the system or application. Related CSRs: 7.3.5, 10.8.2, 10.10.1</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>2.9.7 Password files are encrypted.</p>	<ol style="list-style-type: none"> <li>1. View a sample dump of password files (e.g., hexadecimal printout).</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>FISCAM</p>
<p>Guidance: Encrypting the password file reduces the risk that it could be accessed and read by unauthorized individuals. Related CSRs: 10.5.1</p>		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Access Control**

General Requirement Control Technique	Protocol	Reference
2.9.8 Vendor-supplied passwords are replaced immediately.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM
Guidance: Vendor supplied passwords are known by every hacker and they are usually the first passwords tried by hackers.	Related CSRs: 3.6.2, 10.10.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9.9 Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	<ol style="list-style-type: none"> <li>1. Review pertinent policies and procedures.</li> <li>2. Review documentation of such comparisons.</li> <li>3. Interview security managers.</li> <li>4. Make comparison using audit software.</li> </ol>	FISCAM
Guidance: Policies and procedures should exist for terminating system access for all users no longer requiring access. This does not have to be an automated process but any process that is automatically followed when a user is terminated or transferred.	Related CSRs: 1.10.4, 2.2.20, 2.8.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9.10 Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed periodically--every 30 to 90 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least six alphanumeric characters in length and prohibited from reuse for at least 6 generations.	<ol style="list-style-type: none"> <li>1. Interview users.</li> <li>2. Review security software password parameters.</li> <li>3. Observe users keying in passwords.</li> <li>4. Attempt to log on without a valid password. Make repeated attempts to guess passwords.</li> <li>5. Assess procedures for generating and communicating passwords to users.</li> <li>6. Review pertinent policies and procedures.</li> </ol>	CMS FISCAM HIPAA
Guidance: Policies and procedures should exist that implement these minimum password requirements.	Related CSRs: 7.3.2, 10.10.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9.11 Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords are utilized where supported by existing operating systems.	<ol style="list-style-type: none"> <li>1. Inspect a sample of workstations running each type of operating system in use to confirm that the required process is in use.</li> <li>2. Review configuration documentation supported implementation of the required feature.</li> </ol>	CMS FISCAM HIPAA
Guidance: Workstation time-outs and password protected screen savers are important access controls used to prevent unauthorized users from accessing the system using the logged-on users credentials.	Related CSRs: 7.3.5, 10.10.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
2.9.12 Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.	Review documentation establishing that authorization control exists, and includes the required feature.	HIPAA
Guidance: The mechanisms are used to authenticate users before granting them access permissions to the system or application.	Related CSRs: 2.4.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category:** *Access Control*

<b>General Requirement</b>	<b>Protocol</b>	<b>Reference</b>
<b>Control Technique</b>		
<p>2.9.13 If a CMS business partner is part of a larger organization, the business partner must implement policies and procedures that protect CMS sensitive information from unauthorized access by the larger organization.</p> <p>Guidance: Review security policies and procedures for business partner access.</p> <p style="text-align: center;"> <input type="checkbox"/> <i>SS</i>      <input type="checkbox"/> <i>PartB</i>      <input type="checkbox"/> <i>PartA</i>      <input type="checkbox"/> <i>Dmerc</i>      <input type="checkbox"/> <i>DC</i>      <input type="checkbox"/> <i>CWF</i> </p>	<p>1. Review relevant policies and procedures for inclusion and directed use of the required process.</p> <p>2. Interview a sample of users to confirm the required understanding and access authorizations.</p> <p style="text-align: right;">Related CSRs:</p>	HIPAA
<p>2.10 Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure.</p> <p>2.10.1 Security software is used to restrict access. Access to security software is restricted to security administrators only.</p> <p>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.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>	<p>1. Review documentation describing the security software in use for restriction of access to data files and software programs.</p> <p>2. Review relevant policies and procedures for inclusion and directed use of the required process.</p> <p>3. Review documentation of security software parameters that limit access to the security software to security administrators.</p> <p style="text-align: right;">Related CSRs: 3.6.4, 3.6.5</p>	FISCAM
<p>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.</p> <p>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.</p> <p style="text-align: center;"> <input type="checkbox"/> <i>SS</i>      <input type="checkbox"/> <i>PartB</i>      <input type="checkbox"/> <i>PartA</i>      <input type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>	<p>1. Review relevant policies and procedures for inclusion and directed use of the required process.</p> <p>2. Perform penetration testing by attempting to access and browse computer resources.</p> <p>3. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.</p> <p>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.</p> <p>5. Review documentation describing the standardized naming conventions in use for resources.</p> <p style="text-align: right;">Related CSRs: 6.4.3, 6.4.4, 2.1.4, 3.6.5, 6.4.1, 6.8.2</p>	FISCAM

**Category: Access Control**

General Requirement Control Technique	Protocol	Reference
2.10.3 Updating of data is restricted to authorized employees.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect the Access Authorization List(s) identifying employees who are authorized to update data.</li> <li>3. Inspect a sample of audit data confirming that the required process is consistently used</li> <li>4. Review documentation of the control used to restrict of data updating to authorized employees.</li> </ol>	CMS
<p>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.</p>		
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
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.	<ol style="list-style-type: none"> <li>1. Review documentation of the process used to provide the specified control over routines that modify the status of a file.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.</li> </ol>	CMS
<p>Guidance: Utilities for file access and related processing need controls in place.</p>		
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
2.10.5 Inactive users accounts are monitored and removed when not needed.	<ol style="list-style-type: none"> <li>1. Review a sample of audit data confirming continued operation of the required control.</li> <li>2. Review documentation describing how the required control is implemented.</li> </ol>	FISCAM
<p>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.</p>		
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
2.11 Logical controls shall be implemented for databases and DBMS software.		
2.11.1 Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	<ol style="list-style-type: none"> <li>1. Review security system parameters.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM
<p>Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners.</p>		
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
2.11.2 Access and changes to DBMS software are controlled.	<ol style="list-style-type: none"> <li>1. Review the controls protecting DBMS software.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM HIPAA
<p>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.</p>		
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Access Control**

General Requirement Control Technique	Protocol	Reference
2.11.3 Use of DBMS utilities is limited.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect the Access Authorization List for DBMS utilities to confirm access is limited to those personnel have an operational requirement for access.</li> </ol>	FISCAM
<p>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.</p> <p style="text-align: right;">Related CSRs:</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
2.11.4 Database management systems (DBMS) and data dictionary controls have been implemented that: (1) restrict access to data files at the logical data view, field and field-value level; (2) control access to the data dictionary using security profiles and passwords; (3) maintain audit trails/logs that allow monitoring of changes to the data dictionary; and (4) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.	<ol style="list-style-type: none"> <li>1. Interview database administrator.</li> <li>2. Test controls by attempting access to restricted files.</li> <li>3. Review pertinent policies and procedures.</li> </ol>	FISCAM
<p>Guidance: Access control settings should be implemented in accordance with the access authorizations established by the resource owners. Data dictionary software, which interfaces with the DBMS and provides a method for documenting elements of a database, may also provide a method of securing data. In addition, use of the DBMS and data dictionary should be protected through the use of logical access controls and audit trails.</p> <p style="text-align: right;">Related CSRs: 6.3.5, 6.6.1, 2.8.2, 2.9.4</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
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.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	IRS 1075 PDD 63
<p>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.</p> <p style="text-align: right;">Related CSRs: 1.4.2, 2.5.3, 2.5.7, 2.7.2</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
2.12.2 Medicare data is not released to outside personnel unless their identity is verified.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	CMS
<p>Guidance: There should be procedures used to verify that outside personnel who request Medicare data are authorized to receive the data before releasing it.</p> <p style="text-align: right;">Related CSRs: 1.3.2, 1.3.8</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Access Control**

General Requirement	Protocol	Reference
Control Technique		
2.13 Suspicious access activity shall be investigated and appropriate action taken.		
2.13.1 SSOs investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.	FISCAM
Guidance: Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations should be investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur, repair any damage. The seriousness of the issue should determine what disciplinary actions might be taken. A good approach is to tie these violations/accidents into performance evaluations.	Related CSRs: 7.1.3, 7.2.2, 7.3.1, 7.3.5, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>	
2.13.2 Violations are summarized and reported to senior management.	1. Interview senior management and personnel responsible for summarizing violations. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect audit data confirming that the required process is consistently used.	FISCAM
Guidance: The frequency and magnitude of security violations and corrective actions taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the entity's operations, and any need for additional controls.	Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>	
2.13.3 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	FISCAM
Guidance: Once it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weakness that allowed the violation to occur and repair any damage that has been done.	Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 3.1.2, 3.1.1, 3.4.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>	
2.13.4 Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	CMS IRS 1075
Guidance: The process of inventorying and documenting missing tapes containing sensitive information should be integrated into the normal business processes of the organization.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>	
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
Guidance: A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard forms should be used and maintained on file to document the users' approvals.	Related CSRs: 1.3.8, 2.8.9	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>	

**Category: Access Control**

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
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:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**3. System Software**

3.1	Inappropriate or unusual activity shall be investigated and appropriate actions taken.		
3.1.1	Policy defines investigation of inappropriate or unusual activity and guidelines for appropriate actions to be taken.	Review system operational policies and guidelines.	FISCAM
Guidance:	The possibility of damage or alteration to the system software, application software, and related data files should be investigated and needed corrective actions taken. For example, policy guideline actions should include notifying the resource owner of the violation.	Related CSRs: 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 2.8.2	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
3.1.2	Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Determine when the last management review was conducted, and analyze their review regarding the intended functioning of software monitoring control techniques and controlling risk.	FISCAM
Guidance:	A good approach is to include the evaluation of the software control techniques in the risk assessment with annual reviews. If there are any suspicious functions or processes occurring then the suspicious event should be investigated immediately.	Related CSRs: 6.3.10, 1.5.5, 1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.9.7, 2.13.3, 4.4.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
3.1.3	The use of privileged system software and utilities is reviewed by technical management.	<ol style="list-style-type: none"> <li>1. Interview technical management regarding their reviews of privileged system software and utilities usage.</li> <li>2. Review documentation supporting technical management reviews.</li> <li>3. Review documentation for system software utilities and verify that technical management has given use approvals.</li> <li>4. Some good questions to ask about privileged system software and utilities are:               <ul style="list-style-type: none"> <li>- Are the system privileges granted to users strictly on need to use basis ?</li> <li>- Are there separate user ID's for performing privileged and normal activities?</li> <li>- Are the login privileges for highly privileged accounts available only from console and terminals situated within the console room ?</li> <li>- Is the audit trail maintained of activities conducted by highly privileged users? How long is it preserved?</li> </ul> </li> </ol>	FISCAM
Guidance:	Privileged access may be used only to perform assigned job duties.	Related CSRs: 1.8.4, 3.3.3, 4.1.3, 4.3.1, 4.6.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

General Requirement Control Technique	Protocol	Reference
<p>3.1.4 Systems programmers' activities are monitored and reviewed.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>Determine that system programmer supervisors are supervising and monitoring their staff.</li> <li>Review documentation supporting the supervising and monitoring of systems programmers' activities.</li> <li>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.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 4.2.1, 4.2.4, 3.2.3, 4.4.2</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.1.5 Systems support alarm features to provide immediate notification of predefined events.</p> <p>Guidance: It is a good practice to have an automated audit system perform the immediate notification.</p>	<ol style="list-style-type: none"> <li>Review security plan to determine use of audit logs and alarms set points.</li> <li>Review audit logs.</li> </ol>	<p>HIPAA</p> <p>Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.2 Policies and techniques shall be implemented for using and monitoring system utilities.</p>		
<p>3.2.1 Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.</p> <p>Guidance: Security training is adjusted to the level of the system programmer's responsibilities.</p>	<ol style="list-style-type: none"> <li>Verify that the appropriate responsibilities have been defined.</li> <li>Interview systems programmers regarding their responsibilities.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 1.1.4</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.2.2 Responsibilities for monitoring use are defined and understood by technical management.</p> <p>Guidance: Security training is adjusted to the level of the technical management's responsibilities.</p>	<ol style="list-style-type: none"> <li>Verify that the appropriate responsibilities are defined.</li> <li>Interview technical management regarding their responsibilities.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 1.1.4</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.2.3 Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.</p> <p>Guidance: It is a good practice to identify access for various programs and utilities, monitoring, and written policies and procedures. As part of the System Security Plan, policies and procedures for using and monitoring the use of system software utilities should be defined and documented.</p>	<ol style="list-style-type: none"> <li>Interview management and systems personnel.</li> <li>Verify the existence and current version of the appropriate policies and procedures.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 3.1.4, 4.4.2</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: System Software**

General Requirement Control Technique	Protocol	Reference
3.2.4 The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	<ol style="list-style-type: none"> <li>1. Determine whether logging occurs and what information is logged.</li> <li>2. Review logs.</li> <li>3. Using security software reports, determine who can access the logging files.</li> </ol>	FISCAM
Guidance: The output report log is a good management tool to assist in tracking the usage of sensitive system utilities. The policy and procedures for the sensitive system utilities are normally depicted in the system security plan.	Related CSRs: 1.9.4, 9.6.5	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>		
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.	<ol style="list-style-type: none"> <li>1. Review pertinent policies and procedures.</li> <li>2. Interview management and system personnel regarding access restrictions.</li> <li>3. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access.</li> <li>4. Attempt to access the operating system and other system software.</li> </ol>	FISCAM
Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses.	Related CSRs: 1.1.8	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>		
3.3.2 Policies and procedures for restricting access to systems software exist and are up-to-date.	<ol style="list-style-type: none"> <li>1. Interview management and systems personnel regarding access restrictions.</li> <li>2. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access.</li> <li>3. Attempt to access the operating system and other system software.</li> <li>4. Review pertinent policies and procedures.</li> </ol>	FISCAM
Guidance: Access to system software is restricted to a few system programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly.	Related CSRs: 1.9.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>		
3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of system programmers were reviewed.	FISCAM
Guidance: Security skill needs are accurately identified and included in job descriptions. The duties from the job description should be compared to the SSO's security access list and the security audit logs. If these functions do not match then management should take corrective action(s). The review memo should be provided to the SSO for inclusion in the System Security Profile.	Related CSRs: 3.1.3, 1.1.2, 2.8.3	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>		
3.3.4 Justification and management approval for access to systems software is documented and retained.	<ol style="list-style-type: none"> <li>1. Interview system manager and security administrator.</li> <li>2. Review appropriate documentation, and verify that it is retained.</li> </ol>	FISCAM
Guidance: The SSO normally maintains an approved Access Control Listing (ACL) for all systems that process or transmit sensitive data. The individual's supervisor provides justification and approval to the SSO. The ACL is part of the System Security Profile.	Related CSRs: 1.9.5	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>		

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.		<ol style="list-style-type: none"> <li>1. Interview data center management about their role in reviewing system software installations.</li> <li>2. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.</li> </ol>	FISCAM			
Guidance:	A good process for monitoring and documenting migration of system software is in the change management process for the organization.		Related CSRs: 9.7.1, 9.8.1, 9.8.2, 9.8.3, 6.5.2, 2.3.1, 2.11.2, 2.13.3, 4.7.6, 6.3.5, 6.3.6, 6.3.10, 6.6.1, 6.7.1, 6.8.1, 10.7.3, 10.10.1			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
3.4.2 Migration of tested and approved system software to production use is performed by an independent library control group.		Interview management, systems programmers, and library controls personnel, and determine who migrates approved system software to production libraries, and whether versions are removed from production libraries.	FISCAM			
Guidance:	A good process for monitoring and documenting the migration of system software is in the change management process for the organization.		Related CSRs: 6.8.2, 4.7.6			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
3.4.3 Vendor-supplied system software is supported by the vendor.		Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.	FISCAM			
Guidance:	A good approach is to include vendor maintenance with the purchase of the software.		Related CSRs:			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
3.4.4 Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.		<ol style="list-style-type: none"> <li>1. Interview management and systems programmers about scheduling and giving advance notices when system software is installed.</li> <li>2. Review recent installations and determine whether scheduling and advance notification did occur.</li> <li>3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.</li> </ol>	FISCAM			
Guidance:	If possible, a good approach to scheduling major installations of system software is during off hours. This creates minimal impact on operations and provides time to back out the installation if errors occur. Notification can be provided several days in advance via email.		Related CSRs:			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
3.4.5 Outdated versions of system software are removed from production libraries.		Review supporting documentation from a few system software migrations and the removal of outdated versions from production libraries.	FISCAM			
Guidance:	Outdated versions are kept in a library other than the production library. In order to prevent redundant execution of older versions, they should be deleted from production and moved elsewhere. Storage for outdated versions may be part of the Contingency Plan reconstitution efforts.		Related CSRs:			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

**Category: System Software**

General Requirement Control Technique	Protocol	Reference
3.4.6 All system software is current and has current and complete documentation.	<ol style="list-style-type: none"> <li>1. Review documentation and test whether recent changes are incorporated.</li> <li>2. Interview management and system programmers about the currency of system software, and the currency and completeness of software documentation.</li> </ol>	FISCAM
Guidance: An automated version tracking system can assist with tracking the current version of software and the software's documentation.	Related CSRs: 1.9.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
3.5 System software changes shall be authorized, tested and approved before implementation.		
3.5.1 New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation.	<ol style="list-style-type: none"> <li>1. Determine the procedures used to test and approve system software prior to its implementation.</li> <li>2. Select a few recent systems software changes and review audit data confirming that the specified process was followed.</li> <li>3. Review procedures used to control and approve emergency changes.</li> <li>4. Select some emergency changes to system software and test whether the indicated procedures were in fact used.</li> </ol>	FISCAM
Guidance: This should be documented and provided in the Change Management process. Change management standards, proper controls, processes, and procedures will provide for appropriate testing prior to implementation.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
3.5.2 Policies and procedures exist and are up-to-date for identifying, selecting, installing and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.	<ol style="list-style-type: none"> <li>1. Interview management and systems personnel.</li> <li>2. Verify that policies and procedures are current, and contain the required information.</li> </ol>	FISCAM
Guidance: Usually, the change request will contain most of the selecting, installation and cost information.	Related CSRs: 1.9.4, 1.4.1, 1.8.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
3.5.3 Procedures exist for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.	<ol style="list-style-type: none"> <li>1. Review procedures for identifying and documenting system software problems.</li> <li>2. Interview management and systems programmers.</li> <li>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.</li> </ol>	FISCAM
Guidance: A good approach is to automate the software problem tracking processes. Monthly tracking reviews will assist in controlling any issues.	Related CSRs: 1.9.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: System Software**

General Requirement Control Technique	Protocol	Reference
<p>3.5.4 New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.</p> <p>Guidance: A preformatted change request process provides efficiency and assists in the accuracy of the change tracking processes.</p>	<p>1. Determine what authorizations and documentation are required prior to initiating system software changes.</p> <p>2. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.</p>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.5.5 Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.</p> <p>Guidance: Checkpoints and Restart capabilities on jobs will assist in meeting performance goals.</p>	<p>Verify the existence of checkpoint and restart capabilities.</p>	CMS
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.5.6 Procedures exist for controlling emergency changes. These procedures include: (1) authorizing and documenting emergency changes as they occur, (2) reporting the changes for management review, and (3) review of the changes by an independent IT supervisor.</p> <p>Guidance: A good approach is to include emergency procedures in the change management process as well as appropriate procedures in the Contingency Plan</p>	<p>1. Interview an independent IT supervisor who has previously reviewed changes.</p> <p>2. Verify the existence of emergency change procedures.</p> <p>3. Interview system managers.</p>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.</p>		
<p>3.6.1 All accesses to system software files are logged by automated logging facilities.</p> <p>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.</p>	<p>Review sample accesses to system software files to confirm automated logging facilities.</p>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>3.6.2 Vendor-supplied default login IDs and passwords have been disabled.</p> <p>Guidance: Disabling default passwords and removing the obsolete software should be part of enhancing security (hardening) process when new software or systems are installed.</p>	<p>1. Inquire whether disabling has occurred.</p> <p>2. Test for default presence using vendor standard IDs and passwords.</p>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>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.</p> <p>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.</p>	<p>1. Determine what terminals are set up as master consoles and what controls exist over them.</p> <p>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.</p>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**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.	<ol style="list-style-type: none"> <li>1. Obtain a list of all system software on test and production libraries used by the entity.</li> <li>2. Verify that access control software restricts access to system software.</li> <li>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.</li> <li>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.</li> </ol>	FISCAM HIPAA			
Guidance:	Security skill needs are accurately identified and included in job descriptions. After necessary personnel have been identified, then corresponding access control software must be matched and implemented.	Related CSRs: 2.10.1, 1.1.2				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
3.6.5	The operating system is configured to prevent circumvention of the security software and application controls.	<ol style="list-style-type: none"> <li>1. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.</li> <li>2. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.</li> </ol>	FISCAM			
Guidance:	System hardening should be part of operating system installation. Once the system is hardened then the security should be baselined and periodically updated. Additionally, an Intrusion Detection System, when possible, should be implemented for real time monitoring. A Host Intrusion Detection System would assist in preventing circumvention of controls.	Related CSRs: 2.10.1, 2.10.2, 2.2.1, 2.6.2				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
3.6.6	The operating system's operational status and restart integrity is protected during and after shutdowns.	<ol style="list-style-type: none"> <li>1. Interview the system manager.</li> <li>2. Verify the protection of the operating system during and after shutdowns.</li> </ol>	CMS			
Guidance:	A good practice is to have qualified personnel standing by when systems are taken offline and when shutdowns occur. The QA team could provide a standard list for restart.	Related CSRs: 5.2.9				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

**4. Segregation of Duties**

4.1	Formal procedures shall guide personnel in performing their security duties.					
4.1.1	Application run manuals provide instruction on operating specific applications.	<ol style="list-style-type: none"> <li>1. Inspect run manuals for inclusion of the required instructions.</li> <li>2. Employees demonstrate that documentation is understood and adhered to.</li> </ol>	FISCAM			
Guidance:	Manuals should include instructions on job setup, console and error messages, job checkpoints, transaction logs, and restart and recovery steps after system failure.	Related CSRs: 4.1.3				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

**Category: Segregation of Duties**

General Requirement Control Technique	Protocol	Reference
4.1.2 Operators are prevented from overriding file labels or equipment error messages.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing how controls meet the specified requirement.</li> <li>3. Employees demonstrate that documentation is understood and adhered to.</li> </ol>	FISCAM
Guidance: A good approach is to provide periodic training in operating procedures, which should cover operator-prohibited activities.	Related CSRs: 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5	
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.1.3 Detailed, written instructions exist to guide personnel in performing their duties. Computer operator manuals provide guidance on system startup and shut down procedures, emergency procedures, system and job status reporting, and operator prohibited activities. Application-specific manuals provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.	<ol style="list-style-type: none"> <li>1. Determine that the required operator and security manuals exist, and that they provide the required documentation.</li> <li>2. Determine that documents are understood and adhered to by staff.</li> </ol>	FISCAM
Guidance: Manuals should contain instructions on all procedures which the employee is expected to perform on a regular basis and in an emergency situation.	Related CSRs: 5.6.2, 9.1.2, 9.3.1, 9.5.1, 9.6.7, 9.6.8, 4.1.1, 3.1.3, 3.1.5	
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.1.4 The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data confirming continuing use of the specified approval process.</li> </ol>	CMS
Guidance: The approval process should be documented and reviewed periodically.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.1.5 Duties in critical control and financial functions are split. (e.g., establish special controls involving more than one person over blank and voided checks.)	<ol style="list-style-type: none"> <li>1. Interview supervisors in the critical control and financial areas.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS
Guidance: Duties should be documented in job descriptions. Appropriate separation of data will assist in preventing fraud. See BPSSM information on fraud protective measures.	Related CSRs:	
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.2 Active supervision and review shall be provided for all personnel.		
4.2.1 All operator activities on the computer system are recorded on an automated history log.	<ol style="list-style-type: none"> <li>1. Determine by review that an automated history log exists on each computer system, and that they record all operator activities.</li> <li>2. Interview supervisors to confirm that supervisors routinely review history log.</li> </ol>	FISCAM
Guidance: The history log serves as an audit trail and should be reviewed routinely by supervisors.	Related CSRs: 2.1.1, 2.6.1, 3.1.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Segregation of Duties**

General Requirement	Control Technique	Protocol	Reference			
4.2.2	Personnel are provided adequate supervision and review, including each shift of computer operations.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data confirming continuing supervision and review in accordance with the documented process.</li> </ol>	FISCAM			
Guidance:	Supervision and review of personnel activities assure that these activities are performed in accordance with prescribed procedures, mistakes are corrected, and computers are used for authorized purposes.	Related CSRs: 1.4.1				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
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.	<ol style="list-style-type: none"> <li>1. Interview supervisors and subordinate personnel to confirm continuing use of the required process.</li> <li>2. Observe system startup.</li> <li>3. Review audit data confirming that only authorized personnel are involved in the system startup operation.</li> <li>4. Review audit data confirming that parameters set during IPL are consistently in accordance with documented procedures.</li> </ol>	FISCAM			
Guidance:	IPL establishes the environment in which the computer operates. System startup should be monitored to ensure that security features are enabled.	Related CSRs:				
	<input type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
4.2.4	Supervisors routinely review the history log and investigate any abnormalities.	<ol style="list-style-type: none"> <li>1. Determine, by review supervisor's job description that this is included in the job description.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review history log for signatures indicating supervisory review.</li> <li>4. Inspect a sample of documentation of the supervisor's investigative process.</li> </ol>	FISCAM			
Guidance:	The history log serves as an audit trail.	Related CSRs: 7.3.1, 7.3.6, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 2.1.1, 2.6.1, 3.1.4, 3.1.1				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
4.3	Job descriptions shall be documented.					
4.3.1	Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	<ol style="list-style-type: none"> <li>1. Review documentation establishing that existing documented job descriptions meet segregation of duty principles.</li> <li>2. Inspect the effective dates of position descriptions to confirm that they are current.</li> <li>3. Confirm by interview of the incumbents that documented job descriptions match actual current responsibilities and duties.</li> </ol>	FISCAM			
Guidance:	HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.	Related CSRs: 3.1.3				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

**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.	<ol style="list-style-type: none"> <li>1. Confirm by review that job descriptions are documented, and that they meet the specified criteria.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM			
Guidance:	HR requires assistance in providing updates to the job descriptions. A good approach is to assist the managers of the HR department.	Related CSRs: 5.1.2				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CSW</i>
<hr/>						
4.4	Management shall review effectiveness of control techniques.					
4.4.1	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM			
Guidance:	A good approach is a documented management review on an annual basis.	Related CSRs: 3.1.2, 2.7.1				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CSW</i>
<hr/>						
4.4.2	Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM			
Guidance:	A periodic employee performance review could be used to demonstrate compliance.	Related CSRs: 3.1.4, 3.2.3				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CSW</i>
<hr/>						
4.5	Physical and logical access controls shall be established.					
4.5.1	Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	Review documentation establishing how physical and logical access controls accomplish the specified restriction.	CMS FISCAM			
Guidance:	This can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities.	Related CSRs: 2.3.1				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CSW</i>
<hr/>						
4.6	Employees shall understand their security duties and responsibilities.					
4.6.1	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview employees to confirm that their job descriptions match their understanding of their duties and responsibilities, and that they carry out those responsibilities in accordance with their job descriptions.	FISCAM			
Guidance:	Employees should have access to their job descriptions and discuss during their performance evaluations.	Related CSRs: 3.1.3				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CSW</i>
<hr/>						
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.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM			
Guidance:	Senior management is responsible for assuring that employees understand their responsibilities.	Related CSRs:				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CSW</i>

**Category: Segregation of Duties**

General Requirement Control Technique	Protocol	Reference
4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.	1. Review documented procedures identifying responsibilities for restricting access by job position in key operating and programming activities to confirm that these responsibilities are clearly defined. 2. Interview a sample of personnel identified as having the specified responsibilities to confirm that the responsibilities assigned are clearly understood and followed. 3. Employees demonstrate that documentation is understood and adhered to.	FISCAM
Guidance: A good approach is to develop a matrix identifying resources in relation to organizational access and job title.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.7 Incompatible duties shall be identified and policies implemented to segregate these duties.		
4.7.1 Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Review approval controls.	FISCAM
Guidance: Compensating controls should be documented.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. No individual has complete control over incompatible transaction processing functions.	1. Review the required analyses for inclusion of the specified elements. 2. Confirm by review that the required analyses reflect current operations.	FISCAM
Guidance: Establish independent organizational groups with defined functions. Functions and related tasks performed by each unit should be documented.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.	1. Review documentation of process design establishing the specified separation of duties. 2. Confirm through interview, observation, and review of job descriptions for a sample of personnel, that these separation of duties requirements are met. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	FISCAM
Guidance: Policy procedures and access approvals need to account for correct users of information systems. The initiating approval form can identify job descriptions that are involved for system and application access.	Related CSRs:	
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.7.4 Policies and procedures for segregating duties exist and are up-to-date.	Confirm through inspection that the required policies and procedures exist and are consistent with current operations.	FISCAM
Guidance: Policies are documented, communicated, and enforced.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
4.7.5 Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Confirm by review that documented operating procedures meet the required criteria.	FISCAM
Guidance: Documentation should be reviewed periodically and updated as needed.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Segregation of Duties**

General Requirement	Control Technique	Protocol	Reference
4.7.6	Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) quality assurance/testing; (6) library management/change management; (7) computer operations; (8) production control and scheduling; (9) data control; (10) data security; (11) data administration; and (12) network administration.	<ol style="list-style-type: none"> <li>1. Review the agency organization chart showing IS functions and assigned personnel.</li> <li>2. Interview selected personnel and determine whether functions are appropriately segregated.</li> <li>3. Review relevant alternative or backup assignments and determine whether the proper segregation of duties is maintained.</li> <li>4. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.</li> </ol>	FISCAM
Guidance: Manuals and job descriptions include support functions of each individual.		Related CSRs: 3.4.1, 3.4.2, 3.5.4, 3.5.5	
		<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF	

**5. Service Continuity**

5.1 Adequate environmental controls shall be implemented.

5.1.1	Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known.	<ol style="list-style-type: none"> <li>1. Examine facility maintenance records for history of water damage.</li> <li>2. Interview site managers for knowledge of potential pumping related hazards and familiarity with mitigation procedures.</li> <li>3. Interview a sample of operations staff to confirm familiarity with mitigation procedures for potential plumbing related problems.</li> <li>4. Observe the operation, location, maintenance, and access to the air cooling systems condensate drains.</li> <li>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.</li> <li>6. Review relevant procedures for inclusion mitigation measures for any potential plumbing related problems.</li> <li>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.</li> </ol>	FISCAM
Guidance: The SSO should work in conjunction with the building engineer/maintenance.		Related CSRs:	
		<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF	

5.1.2	Any behavior that may damage computer equipment is prohibited.	<ol style="list-style-type: none"> <li>1. Review the risk assessment for identification of potentially hazardous employee activities.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment.</li> <li>3. Review job descriptions to ensure there is guidance contained relative to destructive behavior.</li> </ol>	FISCAM
Guidance: Management should include behavioral guidance. For example keeping cans of coke on top of a PC could damage it.		Related CSRs: 4.3.2	
		<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF	

**Category: Service Continuity**

General Requirement Control Technique	Protocol	Reference
5.1.3 Controls have been implemented to mitigate other disasters, such as floods, earthquakes and fire.	<ol style="list-style-type: none"> <li>1. Review the risk assessment plan for consideration of the specified potential risks.</li> <li>2. Review documentation of efforts to identify additional risks specific to the region, area, or facility.</li> <li>3. Review documentation of risk mitigation planning covering all identified risks.</li> <li>4. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.</li> </ol>	FISCAM
Guidance: The SSO should work in conjunction with the building engineer/maintenance. High risk items should be identified e.g., location of the flood plain.		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.1.4 Environmental controls are periodically tested.	<ol style="list-style-type: none"> <li>1. Review the test plans for future tests.</li> <li>2. Review test policies.</li> <li>3. Review documentation supporting recent tests of environmental controls.</li> </ol>	FISCAM
Guidance: There should be a test plan for the testing of the environmental controls, e.g., humidistat. Related CSRs: 5.7.1		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.1.5 Redundancy exists in the air cooling system.	<ol style="list-style-type: none"> <li>1. Review facility design documentation confirming air cooling system redundancy.</li> <li>2. Review maintenance records confirming primary and redundancy systems are operational.</li> <li>3. Observe demonstrations of operation of primary and redundant cooling systems.</li> <li>4. Review policy and procedures relevant to operation and maintenance of primary and redundancy air cooling systems</li> </ol>	FISCAM
Guidance: Only the critical components or subsystems of the entire air cooling system need to be redundant. Related CSRs:		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.1.6 Fire suppression and prevention devices have been installed and are working (e.g., smoke detectors, fire extinguishers and sprinkler systems).	<ol style="list-style-type: none"> <li>1. Review facility drawings and other documentation documenting types and locations of the specified devices.</li> <li>2. Review documentation of periodic inspections and maintenance of the specified devices and related systems to assure they are fully operational.</li> <li>3. Review documentation supporting the qualifications of personnel inspecting and maintaining the specified devices and systems.</li> <li>4. Observe that fire extinguishers, smoke detectors and sprinkler systems are in place and appear to be in working order.</li> </ol>	FISCAM
Guidance: A good approach is to have the fire department review the systems. Related CSRs:		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

Category: *Service Continuity*

General Requirement	Protocol	Reference
Control Technique		
5.1.7 An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down.	<ol style="list-style-type: none"><li>1. Review facility documentation confirming installation of an uninterruptible power system (UPS).</li><li>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.</li><li>3. Review documentation supporting existence of periodic test, and preventive maintenance consistent with system specifications.</li><li>4. Review policies and procedures for orderly shut down of the system within the time allowed by the available UPS capacity.</li><li>5. Interview a sample of operations personnel for familiarity with the orderly shut down process and applicable documented procedures.</li><li>6. Review documentation supporting periodic test of the orderly shut down process.</li><li>7. Observe that secondary power supplies exists.</li></ol>	FISCAM
Guidance: The facility managers should periodically verify the current computing power load and auxiliary requirements for change. Related CSRs: 5.9.8, 5.10.1		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2 A Contingency Plan shall be documented in accordance with CMS Contingency Plan Methodology.		
5.2.1 The Contingency Plan provides for backup personnel so that it can be implemented independent of specific individuals.	<ol style="list-style-type: none"><li>1. Review the contingency plan to confirm inclusion of the specified provision.</li><li>2. Review documentation supporting timely availability of the backup personnel required by the contingency plan.</li><li>3. Talk with a random small sample of the designated backup persons to ensure that they understand their role in a contingency.</li></ol>	FISCAM
Guidance: Refer to Appendix B of the BPSSM. Related CSRs: 5.8.1, 5.10.3		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Service Continuity**

General Requirement Control Technique	Protocol	Reference
5.2.2 User departments have developed adequate manual processing procedures for use until automated operations are restored.	<ol style="list-style-type: none"> <li>1. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation.</li> <li>2. Review the contingency plan for identification of the specified manual procedures.</li> <li>3. Inspect the required manual procedures for consistency with the contingency plan.</li> <li>4. Interview the relevant process managers to confirm familiarity with the required procedures.</li> <li>5. Review test reports to determine that manual procedures have been tested, at least on a sample basis.</li> </ol>	FISCAM
Guidance: Determine that the manual procedures have been tested. Refer to Appendix B of the BPSSM.	Related CSRs: 1.8.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.3 The Contingency Plan clearly assigns responsibilities for recovery.	Review the Contingency Plan to confirm clear identification of specific responsibilities for all elements of recovery.	FISCAM
Guidance: Ensure that individuals have been assigned to all the responsibilities that need to be executed during a contingency. Refer to Appendix B of the BPSSM.	Related CSRs: 3.6.4, 4.3.1, 4.6.1, 5.6.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.4 Contingency Plan consists of all components listed in the CMS Business Partner's Systems Security Manual.	<ol style="list-style-type: none"> <li>1. Review Appendix C of the Business Partners Systems Security Manual.</li> <li>2. Verify through inspection that the Contingency Plan includes the specified elements.</li> </ol>	CMS FISCAM HIPAA
Guidance: A business partner contingency plan contains the topics described in Appendix B of the Business Partners Systems Security Manual.	Related CSRs: 5.3.1, 5.4.1, 5.4.2, 5.5.1, 5.6.1, 5.8.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.5 Management and the SSO approve Contingency Plans.	<ol style="list-style-type: none"> <li>1. Verify through inspection that all Contingency Plans have been approved by management and the SSO.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	CMS FISCAM
Guidance: It is important that the contingency plan be reviewed and approved by persons that are knowledgeable about the systems and environment so that nothing is missed in the plan.	Related CSRs: 5.7.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.6 Management and the SSO are able to show how the organization responds to specific disasters/disruptions to: (1) protect lives, (2) limit damage, (3) protect sensitive data, (4) circumvent safeguards according to established bypass procedures, and (5) minimize the impact on Medicare operations.	<ol style="list-style-type: none"> <li>1. Review documentation, CCTV tapes or other recordings.</li> <li>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.</li> </ol>	CMS FISCAM
Guidance: A good approach might be to review documentation in the security profile to determine if the organization has responded properly to emergency situations (such as incidents) in the past.	Related CSRs: 5.5.1, 5.6.1, 5.6.2, 5.6.3, 5.6.4, 5.10.1, 2.6.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Service Continuity**

General Requirement		Protocol	Reference
Control Technique			
5.2.7	The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.  Guidance: Ensure that this immediate entry action has been practiced during exercises and training.	Review the Contingency Plan emergency response procedures for inclusion of the required provision.  Related CSRs: 1.1.7, 2.4.1, 2.4.2, 5.6.1, 5.6.4, 2.2.2	CMS HIPAA
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.8	Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency plans are re-evaluated before proposed changes are approved.  Guidance: Change control management should provide for updates to the Contingency Plan.	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.  Related CSRs:	CMS
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.9	Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.  Guidance: Throughout documentation review and testing, ensure that the safeguards protect data from modification if the system fails.	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.  Related CSRs: 2.5.1, 2.14.2, 3.6.6, 6.4.1, 7.2.2, 9.3.3, 9.8.1, 5.11.2	CMS
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.2.10	The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.  Guidance: Critical interfaces should be tested when the contingency plan is exercised.	1. Review test reports.  2. Verify through inspection that the contingency plan identifies the specified interfaces.  Related CSRs:	CMS
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
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.  Guidance: It is important to know what critical data and operations are needed to continue critical functions in an emergency.	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.  Related CSRs: 1.9.7, 2.1.3, 5.4.4, 5.8.1	FISCAM HIPAA
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Service Continuity**

General Requirement	Control Technique	Protocol	Reference			
5.4 Data and program backup procedures shall be implemented.						
5.4.1 System and application documentation are maintained at the off-site storage location.		<ol style="list-style-type: none"> <li>1. Interview persons at the primary site who are responsible for storing documents off-site.</li> <li>2. Review documentation supporting maintenance of the required off-site storage.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM			
Guidance: Current systems and applications documentation should be available off-site in case the primary processing site is disabled.		Related CSRs: 5.7.3				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
5.4.2 Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.		<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data supporting consistent operation of the required rotation.</li> <li>3. Verify by inspection the location of specific backup files.</li> <li>4. Review documentation confirming successful periodic test of the ability to recover using backup files.</li> </ol>	FISCAM HIPAA			
Guidance: Offsite backup files should be current to the point that operations would not be delayed or disrupted if the data or software were suddenly put into operation.		Related CSRs: 5.11.1, 5.9.8				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
5.4.3 The backup storage site is geographically removed from the primary site(s) and protected by environmental controls and physical access controls.		<ol style="list-style-type: none"> <li>1. By inspection, verify that the backup storage facility is consistent with available documentation.</li> <li>2. Review contingency plan test reports or exercise lessons learned reports to determine if the backup site functioned as planned.</li> <li>3. Review documentation confirming that the backup storage site meets the stated requirements.</li> </ol>	FISCAM			
Guidance: It should be verified that the backup site can operate to process critical data and accomplish critical functions to allow business to progress during an emergency.		Related CSRs: 5.11.2				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
5.4.4 The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.		<ol style="list-style-type: none"> <li>1. Observe the initiation of delivery of critical data from the primary site to the off-site facility.</li> <li>2. Review the Contingency Plan to verify that it contains the specified elements.</li> <li>3. Review records of data backups.</li> </ol>	CMS HIPAA			
Guidance: Refer to Appendix B of the BPSSM.		Related CSRs:				
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
5.4.5 A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.		An inventory of all equipment and software should be maintained, including the location and person responsible.	HIPAA			
Guidance: A record should be use to track the movement all resources.		Related CSRs:				
	<input type="checkbox"/> <i>SS</i>	<input type="checkbox"/> <i>PartB</i>	<input type="checkbox"/> <i>PartA</i>	<input type="checkbox"/> <i>Dmerc</i>	<input type="checkbox"/> <i>DC</i>	<input type="checkbox"/> <i>CWF</i>

**Category: Service Continuity**

General Requirement	Control Technique	Protocol	Reference
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.		<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.</li> </ol>	FISCAM HIPAA
Guidance:	Processing priorities should exist for all critical functions and processes to be accomplished during an emergency. These should be periodically reviewed for accuracy.		Related CSRs: 5.3.1, 5.6.4
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.6 Management and staff shall be trained to respond to emergencies.			
5.6.1 Data center staff have received training and understand their emergency roles and responsibilities.		<ol style="list-style-type: none"> <li>1. Interview a sample of data center staff to confirm their understanding of their roles in emergency response procedures.</li> <li>2. Review training records to confirm required training has been conducted, and is consistent with the current procedures.</li> <li>3. Review training plans for future training in emergency actions.</li> </ol>	FISCAM
Guidance:	There should be evidence that the data center staff has periodically received training relative to what to do in an emergency.		Related CSRs: 1.1.7
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.6.2 Emergency procedures are documented.		By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan.	FISCAM HIPAA
Guidance:	Procedures for use in an emergency should exist for automated and manual processes. They should be readily available. Refer to Appendix B of the BPSSM.		Related CSRs: 1.1.7, 2.2.14, 2.4.1, 3.5.6, 4.1.3, 5.2.7, 6.1.2
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.6.3 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.		<ol style="list-style-type: none"> <li>1. Review training records to confirm that the required training has been delivered periodically.</li> <li>2. Review training plans for future training in emergency actions.</li> </ol>	FISCAM
Guidance:	These are procedures primarily for staff and management working in a data processing center environment.		Related CSRs: 1.1.7
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.6.4 Emergency procedures are periodically tested.		<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation confirming completion of the required testing.</li> <li>3. Review future test plans to ensure that the emergency procedures are scheduled to be properly tested.</li> <li>4. Interview data center staff.</li> </ol>	FISCAM HIPAA
Guidance:	Procedures for use during an emergency situation should be tested annually, or whenever major changes are made to the system environment. Refer to Appendix B of the BPSSM.		Related CSRs: 5.2.7, 5.5.1, 5.7.1
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Service Continuity**

General Requirement Control Technique	Protocol	Reference
<p>5.7 The contingency plan shall be annually reviewed and tested.</p> <p>5.7.1 The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.</p>	<ol style="list-style-type: none"> <li>1. Review documentation of annual conduct of the required test.</li> <li>2. Review documentation describing how the testing conditions simulate an emergency or disaster.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>4. Review test plans for upcoming contingency plan testing, including lessons learned from the previous testing.</li> </ol>	<p>CMS FISCAM HIPAA</p>
<p>Guidance: It is advisable to conduct "live tests" of critical system processes to ensure they will function in an emergency.</p>	<p>Related CSRs: 5.6.4, 2.5.9</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>5.7.2 Contingency Plans are reviewed whenever new operations are planned or new safeguards contemplated.</p>	<ol style="list-style-type: none"> <li>1. Review the current contingency plan.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>CMS FISCAM</p>
<p>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.</p>	<p>Related CSRs: 1.9.5, 1.12.2, 3.5.6, 6.3.10</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data supporting consistent annual review, reassessment, and appropriate revision of the contingency plan as specified.</li> <li>3. Review documentation confirming the required off-site distribution and storage.</li> </ol>	<p>CMS FISCAM</p>
<p>Guidance: Current contingency plans should be readily available to key persons during an emergency. Off-site storage will help ensure this availability.</p>	<p>Related CSRs: 5.4.1, 5.9.3</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>5.7.4 Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review distribution records or interview senior management to ensure that they received the latest contingency plan test results and lessons learned information.</li> </ol>	<p>FISCAM</p>
<p>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.</p>	<p>Related CSRs:</p>	
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Service Continuity**

General Requirement Control Technique	Protocol	Reference
5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documents establishing that the contingency plan and related agreements are adjusted as specified.</li> </ol>	FISCAM HIPAA
Guidance: Following contingency plan testing it is advisable to review the test results and make modifications to the plan and related agreements with inside and outside organizations as quickly as possible.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
5.8 Resources supporting critical operations shall be identified.		
5.8.1 Resources supporting critical operations are identified and documented. Types of resources identified include: (1) computer hardware; (2) computer software; (3) computer supplies; (4) system documentation; (5) telecommunications; (6) office facilities and supplies; and (7) human resources.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect documents identifying resources supporting critical operations for inclusion of the specified resource types.</li> </ol>	FISCAM
Guidance: It is important that resources needed to support critical operations during an emergency and recovery time periods be documented for availability to all concerned persons, and that they be reviewed for currency whenever the contingency plan is to be tested.	Related CSRs: 5.3.1, 2.1.3, 5.4.4, 5.9.8	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.		
5.9.1 Senior management periodically: (1) reviews and compares the service performance achieved with the goals; and (2) surveys user departments to see if their needs are being met.	<ol style="list-style-type: none"> <li>1. Interview users.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review the performance records to ensure the goals are clearly stated in writing.</li> </ol>	FISCAM
Guidance: To avoid a break in continuity of service, hardware performance should be evaluated frequently and users polled relative to level of service provided.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
5.9.2 Problems and delays encountered, including the reason and elapsed time for resolution of hardware problems, are recorded and analyzed to identify recurring patterns or trends.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review samples of the required logs.</li> <li>3. Review documentation supporting conduct of the required analyses.</li> </ol>	FISCAM
Guidance: Hardware problems should be carefully analyzed in order to determine the maintenance needs and to prevent major failures.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
5.9.3 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.</li> </ol>	FISCAM
Guidance: Any changes to hardware equipment or software should be carefully reviewed, tested, and a schedule created for implementation of the changes. Peak workload periods should be avoided for implementation. Vendor supplied specifications normally prescribe the frequency and type of preventative maintenance to be performed.	Related CSRs: 1.9.1, 5.7.3, 6.3.4, 10.7.3, 6.6.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

Category: *Service Continuity*

General Requirement		Protocol	Reference
Control Technique			
5.9.4	Goals are established by senior management for the availability of data processing and on-line services.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation confirming establishment of the required goals.</li> </ol>	FISCAM
	Guidance: Reasonable data processing goals should be set by management to guide the maintenance and problem analysis relative to hardware performance and availability.		Related CSRs:
		<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>	
5.9.5	Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	<ol style="list-style-type: none"> <li>1. Review records of past advanced notifications.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.</li> </ol>	FISCAM
	Guidance: Notice of at least 2 days should be given to users relative to hardware changes.		Related CSRs: 5.7.3, 10.7.3
		<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>	
5.9.6	Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.</li> </ol>	FISCAM
	Guidance: The operational flow of business functions should be designed to permit unscheduled interruptions without adversely affecting critical processes and deliveries.		Related CSRs: 2.2.24
		<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>	
5.9.7	Records are maintained on the actual hardware performance in meeting service schedules.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect the required records.</li> </ol>	FISCAM
	Guidance: Records should be kept for all critical hardware components in the system, such as mainframe, server, disc unit, tape unit, controllers, front end processors, and operations consoles and workstations.		Related CSRs:
		<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>	
5.9.8	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	<ol style="list-style-type: none"> <li>1. Review documentation confirming availability of spare or backup hardware for support of applications designated as critical or sensitive.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review operations and maintenance documentation to confirm that levels of available backup or spare hardware have been sufficient to support system availability objectives.</li> </ol>	FISCAM
	Guidance: In an emergency, or for unscheduled maintenance, spare and backup hardware units, and the appropriate switchover software, should be available to prevent interruption of critical processes.		Related CSRs: 5.4.2, 5.4.3, 5.10.1, 5.11.1, 5.11.2
		<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CSWF</i>	

**Category: Service Continuity**

General Requirement Control Technique	Protocol	Reference
5.9.9 Hardware maintenance policies and procedures exist and are up-to-date.	<ol style="list-style-type: none"> <li>1. Inspect maintenance policies and procedures.</li> <li>2. Review documentation supporting the contention that the required policies and procedures are up-to-date.</li> <li>3. Interview IT and operations staff to ascertain that they are aware of the procedures and know how to use them.</li> </ol>	FISCAM
Guidance: It is important that hardware maintenance policies and procedures are available to all interested persons or groups. They should know where these documents are located. Related CSRs: 1.9.1, 1.4.1, 1.8.4		
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.9.10 Regular and unscheduled hardware maintenance performed is documented.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review maintenance documentation for conformance with the documented procedures.</li> </ol>	FISCAM
Guidance: Maintenance records are kept and reviewed for trends and lessons learned. They can be organized by type unit or subsystem. Review meetings should be held with major vendors reviewing the statistics. Related CSRs: 1.8.4, 1.9.5		
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.9.11 Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	<ol style="list-style-type: none"> <li>1. Inspect hardware maintenance schedules</li> <li>2. Review documentation supporting the contention that the hardware maintenance schedule complies with vendor specifications.</li> <li>3. Review maintenance records to confirm completion of hardware maintenance in accordance with the schedule.</li> <li>4. Review documentation supporting the contention that the manner of performing maintenance minimizes the impact of maintenance on operations.</li> </ol>	FISCAM
Guidance: Maintenance schedules should be distributed and kept at different locations in the enterprise. Related CSRs:		
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
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.	<ol style="list-style-type: none"> <li>1. Review documentation supporting the contention that alternate facilities have sufficient processing capacity.</li> <li>2. Inspect agreements established to confirm coverage of all identified alternate facilities.</li> <li>3. Review documentation identifying facilities required for alternate data processing and telecommunications.</li> <li>4. Review documentation supporting the contention that alternate facilities are in the required state of readiness.</li> <li>5. Review documentation supporting the contention that alternate facilities are available for use.</li> </ol>	CMS FISCAM
Guidance: Agreements should be such that the services to be provided in an emergency are clearly defined and understood by all parties concerned. Security and protection of information should be addressed in these agreements. Related CSRs: 2.2.27, 5.1.7, 5.4.2, 5.4.3, 5.9.8		
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Service Continuity**

General Requirement Control Technique	Protocol	Reference
5.10.2 Alternate telecommunication services have been arranged.	Review documentation confirming the arrangement of alternate telecommunication services.	FISCAM
Guidance: A careful analysis should be made of all telecommunications utilized in normal times, and the links necessary to support critical functions identified.	Related CSRs: 5.7.5, 5.8.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.10.3 Arrangements are planned for travel and lodging of necessary personnel, if needed.	Verify by inspection that the required arrangements have been planned.	CMS FISCAM
Guidance: Arrangements should address persons that may need to come from distant locations and those that are local but may need to stay at or near the data processing site.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
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
Guidance: Standalone workstations must be protected and contingency plans made for backup of their resident software and data.	Related CSRs: 5.4.2, 1.13.1, 1.13.5, 2.2.12, 7.4.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
5.11.2 Standalone computer workstation backup data, software and current operating procedures are stored in accordance with the Contingency Plan.	1. Review relevant policies and procedures for inclusion and directed use of the required process.  2. Through inspection for a sample of standalone workstations, establish that the specified storage criteria are met.	CMS
Guidance: It is suggested that this back-up information be stored at a location different from the workstations.	Related CSRs: 5.2.9, 5.4.3, 5.4.2, 5.9.8	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
5.12 Detection of malicious software shall be performed.		
5.12.1 The CMS Business Partner shall use special software to accomplish malicious software identification, detection, protection, and elimination.	1. Review relevant policies and procedures for inclusion and directed use of the required process.  2. Confirm by inspection that the required software is installed and operational in accordance with documented policy.	FISCAM HIPAA
Guidance: This special software should be approved and tested by knowledgeable persons before being installed.	Related CSRs: 1.1.1, 1.9.1, 2.2.24, 10.2.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

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

General Requirement	Protocol	Reference
Control Technique		

**6. Application Software Development and Change Control**

6.1 Emergency changes to application software shall be promptly tested and approved.

6.1.1 Emergency changes are documented and approved by appropriate operations management, formally reported to appropriate computer operations management for follow-up, and approved after the fact by appropriate programming and user management.

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

FISCAM

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

Related CSRs: 6.3.2, 6.6.1

SS       PartB       PartA       Dmerc       DC       CWF

6.1.2 Emergency change procedures are documented.

Review the documentation of emergency change procedures.

FISCAM

Guidance: Ensure that the procedures for making emergency software changes are current.

Related CSRs: 1.1.7, 2.4.1, 2.4.2, 3.5.6, 5.6.2, 1.9.3, 10.7.3

SS       PartB       PartA       Dmerc       DC       CWF

6.2 Use of public domain and personal software shall be restricted.

6.2.1 Clear policies restricting the use of personal and public domain software have been developed and are enforced.

1. Review the required policies, and verify that they are enforced.
2. Interview the security administrator..
3. Interview users.

FISCAM

Guidance: It may be necessary to periodically randomly inspect disk drives and servers to ensure that only approved personal or public domain software is resident.

Related CSRs:

SS       PartB       PartA       Dmerc       DC       CWF

6.3 Changes shall be controlled as programs progress through testing to final approval.

6.3.1 Test plans are documented and approved that define responsibilities for each party involved.

1. Interview test manager, and others as deemed necessary.
2. Interview the system manager.
3. Verify that test plans are documented and approved, and define the required responsibilities.

FISCAM

Guidance: Persons involved in testing may include system analysts, programmers, quality assurance analysts, data base managers, security analyst, network analyst, software library control staff, users, system administrators, and test planners.

Related CSRs: 2.5.11

SS       PartB       PartA       Dmerc       DC       CWF

6.3.2 Unit, integration and system testing are performed and approved in accordance with the test plan. A sufficient range of valid and invalid conditions are applied.

1. For the software change request selected: (1) Compare test documentation with related test plans; (2) Analyze test failures to determine if they indicate ineffective software testing.
2. Review test plan to ensure that it addresses test levels and conditions.

FISCAM

Guidance: The test plan should be carefully reviewed to ensure that all necessary levels of testing are described and that test conditions are clearly defined. Test standards should be available.

Related CSRs: 2.5.10, 2.5.11, 3.5.1

SS       PartB       PartA       Dmerc       DC       CWF

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

General Requirement Control Technique	Protocol	Reference
<p>6.3.3 A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live test data are not to be used in testing.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Confirm the restrictions in the use of live data.</li> <li>2. Interview test programmers.</li> <li>3. Interview the system manager.</li> <li>4. Verify that test data will meet all processing criteria.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 1.9.1, 2.5.10, 2.5.11, 3.5.1, 4.7.6, 5.9.3, 6.4.4, 9.8.1</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
<p>6.3.4 Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.</p> <p>Guidance: Documentation used by hardware, software, operations, and systems persons should reflect the latest system and software environment.</p>	<ol style="list-style-type: none"> <li>1. Review documentation of all required departments for prompt and accurate updating.</li> <li>2. Interview the system manager.</li> <li>3. Interview the document control person (librarian).</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 1.9.1, 1.9.7, 2.5.1, 2.5.10, 3.4.6, 5.4.1, 5.8.1, 6.5.1, 5.9.3, 1.9.3, 10.7.3</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
<p>6.3.5 Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Interview the software programming supervisor.</li> <li>2. Review documented software changes to verify the tracing process.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 2.11.2, 2.11.4, 3.5.6, 6.1.1, 6.6.1, 10.7.3, 6.7.2, 3.4.1</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
<p>6.3.6 Program changes are moved into production only upon documented approval from users and system development management.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Interview user management.</li> <li>2. Verify the documented approval of program changes before production implementation.</li> <li>3. Interview system development management.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 3.4.5, 3.4.1</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
<p>6.3.7 Test results are reviewed and documented.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Verify that test results are reviewed and documented.</li> <li>2. Interview the system manager.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 2.5.10</p>
<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		

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

General Requirement Control Technique	Protocol	Reference
6.3.8 Changes to detailed system specifications are prepared by the programmer and reviewed by the appropriate supervisor or manager.	1. Interview the programming supervisor. 2. Review documented changes to system specifications.	FISCAM
Guidance: Specification changes are very important and can have far reaching effects. The requests for these should be carefully reviewed and approved by knowledgeable persons.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
6.3.9 Test plan standards have been developed and are followed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).	1. Ensure through observation or interviews that during testing persons/groups fulfilled their responsibilities. 2. Review test plan standards, and confirm that they follow all levels of testing and responsibilities. 3. Interview department supervisors to verify their compliance with test plan standards.	FISCAM
Guidance: A good practice is to have independent tests performed.	Related CSRs: 1.4.4, 2.5.11	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
6.3.10 Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	1. Interview the system programmers and/or system administrator. 2. Determine when the last production program change was reviewed, and how often. 3. Interview data center management and/or the security administrator.	FISCAM
Guidance: Access controls and change controls should be periodically reviewed and/or tested to ensure their proper function.	Related CSRs: 3.1.2, 3.1.3, 3.3.3, 3.4.1, 4.4.1, 7.3.6	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
6.3.11 A system development life cycle (SDLC) methodology has been developed that: (1) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (2) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; and (3) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements.	1. Interview the system manager. 2. Confirm that the SDLC includes the three required elements.	FISCAM
Guidance: Ensure that a current SDLC methodology exists, addresses security has been reviewed, and is being followed.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
6.3.12 Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	1. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current. 2. Examine training plans and records. 3. Interview the programming staff and the software staff.	FISCAM
Guidance: Training plans and materials should exist for training in SDLC methodology.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

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

General Requirement	Control Technique	Protocol	Reference			
6.3.13	Security policy assigns responsibility to Application System Managers for ensuring that appropriate administrative, physical and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.	<ol style="list-style-type: none"> <li>1. Interview system programmers and administrators.</li> <li>2. Interview the application system managers.</li> <li>3. Review the documented policy to ensure that the required responsibilities are assigned.</li> </ol>	CMS HIPAA			
Guidance:	Tests should be performed and test reports should be reviewed to ensure that safeguards that protect software from unauthorized modification have been tested.	Related CSRs: 1.5.2, 1.5.6, 1.9.5, 5.7.2				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
6.4	Access to program libraries shall be restricted.					
6.4.1	Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features.	<ol style="list-style-type: none"> <li>1. For critical software production programs, determine whether access control software rules are clearly defined.</li> <li>2. Determine if the access controls are implemented and working.</li> </ol>	FISCAM HIPAA			
Guidance:	Separate software libraries should be established and only the library control group should be allowed move programs between libraries. Programmers should only have access to the programs they are assigned.	Related CSRs: 5.2.9, 1.4.4, 1.5.6, 2.8.6, 3.3.1, 10.10.1, 2.10.2				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
6.4.2	All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	Select a few program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tape.	FISCAM			
Guidance:	The tape log should be protected from exposure to unauthorized changes or release.	Related CSRs: 1.3.12, 2.2.8, 2.2.23, 2.8.6				
	<input type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
6.4.3	Production source code is maintained in a separate archive library.	<ol style="list-style-type: none"> <li>1. Monitor libraries in use.</li> <li>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.</li> </ol>	FISCAM			
Guidance:	The separate archive library should be protected from unauthorized access by software or physical controls.	Related CSRs: 2.10.2				
	<input checked="" type="checkbox"/> SS	<input type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input type="checkbox"/> CWF
6.4.4	Separate libraries are maintained for program development and maintenance, testing, and production programs.	<ol style="list-style-type: none"> <li>1. Interview library control personnel.</li> <li>2. Monitor libraries in use.</li> </ol>	FISCAM			
Guidance:	The separate libraries should each have their own set of access controls so that, for example, testers cannot access production code.	Related CSRs: 2.10.2, 3.4.5, 6.8.2				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
6.5	Distribution and implementation of new or revised software shall be controlled.					
6.5.1	Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.	<ol style="list-style-type: none"> <li>1. Examine procedures for distributing new software.</li> <li>2. Check implementation orders for a sample of changes.</li> </ol>	FISCAM			
Guidance:	The implementation order should leave no doubt as to when the new software should start to be used for production.	Related CSRs: 1.9.5, 3.5.1, 6.3.4				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF

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

General Requirement	Control Technique	Protocol	Reference
6.5.2	Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.	FISCAM
Guidance:	Software should be distributed allowing enough time at the site for installation, testing, and migration to production.	Related CSRs: 1.9.1, 2.11.2, 3.1.3, 3.4.1, 3.4.4, 3.5.4, 10.7.2	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
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.	<ol style="list-style-type: none"> <li>1. Interview personnel responsible for library control.</li> <li>2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures.</li> <li>3. Review software change control policies and procedures.</li> </ol>	FISCAM
Guidance:	Software controls should be easily monitored and audited. Library management of software helps ensure that differing versions are not accidentally misidentified.	Related CSRs: 6.3.5, 2.11.2, 2.11.4, 3.5.4, 3.5.6, 5.9.3, 6.1.1, 6.3.5, 10.7.3, 10.10.1, 6.8.2, 3.4.1	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
6.7	Authorizations for software modifications shall be documented and maintained.		
6.7.1	Change requests are approved by both system users and data processing staff.	<ol style="list-style-type: none"> <li>1. Determine if the change requests for past changes have been approved.</li> <li>2. Interview software development staff.</li> <li>3. Identify recent software modifications and determine whether change request forms were used.</li> </ol>	FISCAM
Guidance:	A good practice is to convene the change-control board to assure all appropriate personnel provide input and approval for software modifications and document the approval of the proposed changes.	Related CSRs: 3.5.4, 3.4.1	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
6.7.2	Software change request forms are used to document requests and related approvals.	Examine a selection of software change request forms for approvals.	FISCAM
Guidance:	The forms should be designed such that they help ensure that change requests are clearly communicated. The authorization form may be maintained as a paper or softcopy item.	Related CSRs: 3.3.4, 6.3.5	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
6.8	Movement of programs and data among libraries shall be controlled.		
6.8.1	Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.	<ol style="list-style-type: none"> <li>1. Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared.</li> <li>2. Examine some of the images of stored code that has been changed.</li> </ol>	FISCAM
Guidance:	An independent library control group should make the image comparisons.	Related CSRs: 3.4.1	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>

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

<b>General Requirement</b>	<b>Control Technique</b>	<b>Protocol</b>	<b>Reference</b>
6.8.2	A group independent of the user and programmers controls movement of programs and data among libraries.	Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.	FISCAM
Guidance:	Prior to moving software from a test to production environment, an independent review of the changes developed and tested should be made.	Related CSRs: 2.10.2, 3.4.2, 6.3.9, 6.4.2, 6.4.4, 6.6.1	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>

**7. Application System Authorization Controls**

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

7.1.1	For batch application systems, a batch control sheet is prepared for a group of source documents and includes; date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.	<ol style="list-style-type: none"> <li>1. Review the documented procedure for batch control sheet preparation.</li> <li>2. Check a sample of batch control sheets to ensure the inclusion of the Control Technique elements.</li> </ol>	FISCAM
Guidance:	A preformatted batch control sheet will simplify the tracking process for batch application systems or interactive systems with batching capabilities.	Related CSRs:	
	<input type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>

7.1.2	Access to blank documents (checks, claims forms, etc.) is restricted to authorized personnel.	<ol style="list-style-type: none"> <li>1. Interview a sample of personnel to confirm use of documented handling procedures.</li> <li>2. Inspect blank document storage access controls for conformance to documented policy.</li> <li>3. Review documented procedure containing authorized names and control of access.</li> </ol>	FISCAM
Guidance:	It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents.	Related CSRs: 1.1.8	
	<input type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>

7.1.3	Source documents (checks, claims forms, etc.) are pre-numbered to maintain control over the documents. Key source documents require authorizing signatures.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Confirm that documents contain authorized signatures.</li> <li>3. Review the documented procedure for recording and tracking of document numbers.</li> <li>4. Review documentation identifying "key source documents".</li> </ol>	FISCAM
Guidance:	It is a good practice to have the SSO validate the authorization list of those personnel designated to handle sensitive blank documents. Pre-numbered documents help/prevents missing or lost documents.	Related CSRs: 2.6.1, 2.13.1	
	<input type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>

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.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
Guidance:	It is a good practice to verify the transaction is applicable before any transactions are processed. For example, a procurement system requires approved vendors prior to processing of transactions.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>

**Category: Application System Authorization Controls**

General Requirement Control Technique	Protocol	Reference
7.2.2 Master files and program code that does the verification are protected from unauthorized modification.	<ol style="list-style-type: none"> <li>1. Identify and observe the procedures employed that protect master files and program code.</li> <li>2. Review the documented procedure covering the protection of master files and program code.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> <li>4. Review documentation of software controls used in providing the required protection.</li> </ol>	FISCAM
Guidance: The organization should maintain an application protection policy regarding the protection and modification of application master files and program code. A recommendation could be to include the policy in the application change management process or part of the organization's security profile.	Related CSRs: 5.2.9, 2.6.1, 2.13.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
7.3 Data entry workstations shall be secured and restricted to authorized users.		
7.3.1 All transactions are logged as entered, along with the User ID of the person entering the data.	<ol style="list-style-type: none"> <li>1. Observe the processing of sample transactions, to ascertain that they are being logged correctly.</li> <li>2. Review the documented procedure prescribing transaction logging.</li> </ol>	FISCAM
Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the data entry process is correct.	Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
7.3.2 Each operator is required to use a unique password and identification code before being granted access to the system.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Review documented login procedure.</li> <li>3. Observe a sample of data entry login.</li> </ol>	FISCAM
Guidance: Training curriculum includes information on the restrictions against unauthorized activities and accesses, including the use of password and identification control.	Related CSRs: 2.9.10	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
7.3.3 When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Observe physical area during non-business hours.</li> </ol>	FISCAM
Guidance: Review the workstation policy/guidelines.	Related CSRs: 1.13.1, 2.2.12	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
7.3.4 Data entry workstations are connected to the system only during specific periods of the day, which corresponds with the business hours of the data entry personnel.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review documented procedure for workstation use.</li> <li>3. Observe workstation use.</li> </ol>	FISCAM
Guidance: Review the workstation policy/guidelines.	Related CSRs: 1.13.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

**Category: Application System Authorization Controls**

General Requirement Control Technique	Protocol	Reference
7.3.5 Each workstation automatically disconnects from the system when not used after a specific period of time.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review documented procedure for workstation configuration and use.</li> <li>3. For a sample of workstation types, observe operation of the automatic disconnect process.</li> </ol>	CMS FISCAM
Guidance: Review the workstation policy/guidelines. Additionally, it is a good practice to review the audit logs to validate the workstation disconnect functionality.	Related CSRs: 1.13.1, 2.6.1, 2.13.1, 2.9.11, 2.9.6	
<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF		
7.3.6 Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
Guidance: This is a function of the audit process. It is a good practice to manually review the audit logs to validate that the online access process is correct.	Related CSRs: 6.3.10, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 4.2.4, 8.1.1, 8.2.1, 2.9.1	
<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF		
7.3.7 Data entry workstations are located in physically secure environments.	<ol style="list-style-type: none"> <li>1. Review System Security Plan.</li> <li>2. Observe location of workstations.</li> </ol>	FISCAM
Guidance: Workstations processing or connected to systems processing sensitive data are located in physically secure areas.	Related CSRs: 2.2.12	
<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input type="checkbox"/> DC <input type="checkbox"/> CWF		
7.4 Users shall be limited to a set of authorized transactions.		
7.4.1 Authorization profiles for users limit what transaction data entry personnel can enter.	<ol style="list-style-type: none"> <li>1. Review audit controls used to assure continued application of the required procedure.</li> <li>2. Review documented procedure for data entry to confirm enforcement of the required limitation.</li> </ol>	FISCAM
Guidance: Review the application processing policy/guidelines.	Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4	
<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF		
7.4.2 Authorization profiles for users or workstations limit what transactions can be entered.	<ol style="list-style-type: none"> <li>1. For a sample of each type of restricted workstation, observe attempted entry of a prohibited transaction by a logged on user who has the user permissions required to enter the transaction.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review documentation of configuration management assuring continued operation of the required controls.</li> <li>4. Review documents designating transactions authorized from each workstation.</li> </ol>	FISCAM
Guidance: The supervisors should address limitations in access for inclusion in the ACL.	Related CSRs: 1.13.1, 2.10.3, 2.10.4, 2.9.4	
<input checked="" type="checkbox"/> SS <input checked="" type="checkbox"/> PartB <input checked="" type="checkbox"/> PartA <input checked="" type="checkbox"/> Dmerc <input checked="" type="checkbox"/> DC <input checked="" type="checkbox"/> CWF		

**Category: Application System Authorization Controls**

General Requirement Control Technique	Protocol	Reference
<p>7.5 Exceptions shall be reported to management for review and approval.</p> <p>7.5.1 Exceptions, based on parameters established by management, are reported for their review and approval.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>7.6 Independent reviews of data shall occur before entering the application system.</p> <p>7.6.1 Procedures are in place for a multilevel review of CMS sensitive input data before it is released for processing.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review documented procedure for pre-processing of data.</li> <li>2. Interview a sample of supervisors and control unit personnel to confirm use of the process.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>7.6.2 Data control unit personnel monitor data entry and processing of source documents.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Interview management and data control unit personnel to confirm use of the process.</li> <li>2. Review documented data entry and processing procedures.</li> <li>3. Observe data entry and processing procedures.</li> </ol>	FISCAM
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		
<p>7.6.3 Data control unit personnel verify that source documents are properly prepared and authorized.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Interview management and data control unit personnel to confirm use of the process.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>4. Observe data control unit personnel performing the verification process.</li> </ol>	FISCAM
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		

Category: *Application System Completeness Controls*

General Requirement	Control Technique	Protocol	Reference			
<b>8. Application System Completeness Controls</b>						
8.1 Computer sequence-checking shall be implemented.						
8.1.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.		<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review reports of missing or duplicate transactions.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM			
Guidance:	An alteration to the data files should be investigated and needed corrective actions taken. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation so that timely action(s) can be taken.		Related CSRs: 7.3.1, 7.3.6, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
8.1.2 Sequence checking is used to identify missing or duplicate transactions.		<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM			
Guidance:	The possibility of alterations, missing transactions or duplicate transactions can occur if sequence numbers are not properly processed. If a sequence number is missing it may have been deleted or misplaced. The missing or duplicate data files should be investigated and corrective actions taken. For example, within the CMS policy guidelines, actions should include notifying the resource owner of the violation.		Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4, 8.2.1			
	<input checked="" type="checkbox"/> <i>SS</i>	<input type="checkbox"/> <i>PartB</i>	<input type="checkbox"/> <i>PartA</i>	<input type="checkbox"/> <i>Dmerc</i>	<input type="checkbox"/> <i>DC</i>	<input type="checkbox"/> <i>CWF</i>
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.		<ol style="list-style-type: none"> <li>1. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers.</li> <li>2. Review the documented procedure that prescribes the assigning of unique sequence numbers.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> <li>4. Verify, through 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.</li> <li>5. Interview the system owner and determine what policies and corrective action are in place when a sequence number error occurs.</li> </ol>	FISCAM			
Guidance:	This is a function of the processing application. The application developer or vendor should verify the existence of transaction serial numbers being assigned, and sequence number checking routines or modules included in the application.		Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4			
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

**Category: Application System Completeness Controls**

General Requirement Control Technique	Protocol	Reference
<p>8.1.4 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4</p>
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		
8.2 Computer matching of transaction data shall be implemented.		
<p>8.2.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Verify the application has an assigned system owner.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> <li>4. Verify the application has the ability to insert the preassigned source document numbers matched with the associated data.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 7.3.1, 7.3.6, 8.1.2, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Verify that a system owner has been designated and when errors occur, that person is notified.</li> <li>2. Review the program specifications that describe the computer matching process.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1, 4.2.4, 9.3.5, 9.3.6</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>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.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review the documented procedure that describes the comparison process.</li> <li>2. Verify that a staff person is assigned and responsible for verifying that high-value transaction data accurately reflects data from the source documentation.</li> <li>3. Inspect documentation identifying items designated as high-value, low volume.</li> <li>4. Inspect audit data confirming that the required process is consistently used.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 2.1.3, 2.1.5, 2.1.6</p>
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		

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

<b>General Requirement</b>	<b>Control Technique</b>	<b>Protocol</b>	<b>Reference</b>
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.		<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>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.</li> <li>3. Review the documented procedure describing the reconciliation process.</li> </ol>	FISCAM
Guidance:	This process is application dependent, but should be automated as much as possible.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
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.		<ol style="list-style-type: none"> <li>1. Review the documented procedures for the data entry process.</li> <li>2. Review a sample of data control reports for completeness of data entry.</li> <li>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.</li> </ol>	FISCAM
Guidance:	The application should be tracking each transaction and reconciling any differences with the data being entered. (commonly called "run-to-run control totals")		Related CSRs: 2.1.3, 2.1.5, 2.1.6
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>
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.		<ol style="list-style-type: none"> <li>1. Verify that the application contains routines for process checking. The checking process should be included in applicable trailer labels.</li> <li>2. Interview the supervisory application programmer to determine that system controls are in place as prescribed by the application programs.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> <li>4. Review the program specifications describing the reconciliation process for accurate data entry.</li> </ol>	FISCAM
Guidance:	Trailer labels may include any number of tracking or checking techniques. The Trailer labels verify the accuracy of the process, but not the data entry accuracy. If the data is entered correctly and the data is processed completely, then there should not be errors in the output.		Related CSRs: 2.1.3, 2.1.5, 2.1.6
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>

**Category: Application System Completeness Controls**

General Requirement Control Technique	Protocol	Reference
8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	<ol style="list-style-type: none"> <li>1. Review the documented procedures describing the reconciliation process for data entry.</li> <li>2. Interview the supervisory application programmer to determine implementation of automatic reconciliation in completion of computer job runs.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> <li>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.</li> </ol>	FISCAM
<p>Guidance: This process is largely application dependent, but should be automated as much as possible. If an automated function is not available for the software, then consideration for developing such a process would improve the security of the application. Related CSRs: 2.1.3, 2.1.5, 2.1.6</p>		
<p style="text-align: center;"><input checked="" type="checkbox"/> <i>SS</i>      <input type="checkbox"/> <i>PartB</i>      <input type="checkbox"/> <i>PartA</i>      <input type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
8.4.4 System interfaces require that the sending system's output control counts equal the receiving system's input counts.	<ol style="list-style-type: none"> <li>1. Review the documented procedure describing the reconciliation process between systems.</li> <li>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.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<p>Guidance: As systems have become more integrated over the years, a file produced by one application may be used in another application. It is important to reconcile control information between the sending and receiving applications. Related CSRs: 2.1.3, 2.1.5, 2.1.6</p>		
<p style="text-align: center;"><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
8.4.5 A data processing control group receives and reviews control total reports and determines the completeness of processing.	<ol style="list-style-type: none"> <li>1. Review the documented procedure describing the data control group's function.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<p>Guidance: Performing the comparison of control numbers is commonly referred to as balancing, and should be done automatically by the computer, although some older systems may rely on manual balancing procedures. The control numbers for the balancing at key points should be documented, such as being printed on a control totals report, and should be reviewed by the data processing control group that monitors the completeness and accuracy of processing. Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3</p>		
<p style="text-align: center;"><input type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
<p>8.5 Record counts and control totals shall be implemented on an IT System.</p>		
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.	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review the documented procedures for the data control and data entry process for inclusion of the required process.</li> </ol>	FISCAM
<p>Guidance: This is part of the quality assurance process. Since the processing is on-line or real-time, the system can not be taken down for validation of processing. The only way to validate the processing accuracy is to take a snap shot or monitor the processing for accuracy by taking a sampling over a period of time. Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3</p>		
<p style="text-align: center;"><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input type="checkbox"/> <i>CWF</i></p>		

**Category: Application System Completeness Controls**

General Requirement	Control Technique	Protocol	Reference			
8.5.2	User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.	<ol style="list-style-type: none"> <li>1. Inspect the process and documents for developing record counts and control totals to determine data entry completeness.</li> <li>2. Review the documented procedures for the data control process.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM			
Guidance:	In general, user-prepared totals established over source documents and data to be entered can be carried into and through processing. The computer can generate similar totals and track the data from one processing stage to the next and verify that the data was entered and processed as it should have been.	Related CSRs: 2.1.3, 2.1.5, 2.1.6, 7.6.2, 7.6.3				
	<input type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input type="checkbox"/> DC	<input type="checkbox"/> CWF

**9. Application System Accuracy Controls**

9.1 Erroneous data shall be reported back to the user departments for investigation and correction.

9.1.1	Errors are corrected by the user originating the transaction.	<ol style="list-style-type: none"> <li>1. Interview a sample of supervisors and subordinate personnel to confirm use of the documented procedure.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> <li>3. Review the documented error correction procedure.</li> </ol>	FISCAM			
Guidance:	Some systems may use error reports to communicate to the user department the rejected transactions in need of correction. More modern systems will provide user departments access to a file containing erroneous transactions. Using a computer terminal or workstation, users can initiate corrective actions. The user responsible for originating the transaction should be responsible for correcting the error.	Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6				
	<input type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input type="checkbox"/> DC	<input type="checkbox"/> CWF

9.1.2	Error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	<ol style="list-style-type: none"> <li>1. Interview a sample of supervisors and subordinate personnel to confirm that all specified reports and files have the required characteristics..</li> <li>2. Review sample error reports/files, and confirm that error messages contain the information specified in the Control Techniques.</li> <li>3. Review the documented error processing procedure.</li> </ol>	FISCAM			
Guidance:	A good approach to tracking errors and developing procedures to minimize errors would be a detailed error list for managers and supervisors to track and expand corrective actions. Error messages should clearly indicate what the error is and what corrective action is necessary.	Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1				
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF

9.1.3	All corrections are reviewed and approved by supervisors before the corrections are reentered. (Based on Medicare operating environment CMS Business Partners may have other compensating controls in place.)	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review the documented error correction procedure for inclusion of the required process.</li> <li>3. Interview a sample of supervisors and subordinate personnel to confirm use of the required process.</li> </ol>	FISCAM			
Guidance:	As part of the formal security program, policies should be in a procedures document with system security features for error-correction procedures included. All corrections should be reviewed and approved by supervisors before being reentered into the system, or released for processing if corrected from a computer terminal or workstation.	Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6				
	<input type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA	<input checked="" type="checkbox"/> Dmerc	<input type="checkbox"/> DC	<input type="checkbox"/> CWF

**Category: Application System Accuracy Controls**

General Requirement	Control Technique	Protocol	Reference
9.2	Automated entry devices shall be used to increase data accuracy.		
9.2.1	Effective use is made of automated entry devices to reduce the potential for data entry errors.  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.	Review the documentation explaining how the specified objective is met.  Related CSRs: 2.2.16	FISCAM
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA
	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input type="checkbox"/> CWF
9.3	Rejected transactions shall be controlled with an automated error suspense file.		
9.3.1	Rejected data are automatically written on an automated suspense file and held until corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error; (2) date and time the transaction was processed and the error identified; and (3) the identity of the user who originated the transaction.  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.	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.  Related CSRs: 9.1.2, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.1, 9.3.6, 9.7.1, 9.5.1, 9.6.7, 9.6.8, 3.1.5	FISCAM
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA
	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input checked="" type="checkbox"/> CWF
9.3.2	A control group is responsible for controlling and monitoring rejected transactions.  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.	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.  Related CSRs:	FISCAM
	<input type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA
	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input type="checkbox"/> CWF
9.3.3	General controls effectively protect the suspense file from unauthorized access and modification.  Guidance: General controls should protect the suspense file from unauthorized access and modification, in order for the auditor to be able to rely on this control technique to reduce audit risk. A good approach would be to document the security features of the system, spelling out system monitoring characteristics and the action taken when policies are not followed.	Review the documentation describing how general controls provide the required protection of the suspense file.  Related CSRs: 5.2.9, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6	FISCAM
	<input checked="" type="checkbox"/> SS	<input checked="" type="checkbox"/> PartB	<input checked="" type="checkbox"/> PartA
	<input checked="" type="checkbox"/> Dmerc	<input checked="" type="checkbox"/> DC	<input type="checkbox"/> CWF
9.3.4	The suspense file is purged of transactions as they are corrected.  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.	1. Review the documented procedure for the error correction process to confirm inclusion of the specified process. 2. Inspect audit data confirming that the required process is consistently used.  Related CSRs: 2.8.2	FISCAM
	<input checked="" type="checkbox"/> SS	<input type="checkbox"/> PartB	<input type="checkbox"/> PartA
	<input type="checkbox"/> Dmerc	<input type="checkbox"/> DC	<input type="checkbox"/> CWF

**Category: Application System Accuracy Controls**

General Requirement Control Technique	Protocol	Reference
9.3.5 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.	<ol style="list-style-type: none"> <li>1. Review the documented procedure for suspense file processing and transaction reconciliation.</li> <li>2. Observe the suspense file process to confirm that the documented procedure is followed.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<p>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.</p>	Related CSRs: 8.2.2	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
9.3.6 The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected errors.	<ol style="list-style-type: none"> <li>1. Review the documented suspense file procedure for inclusion of the specified processes.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<p>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.</p>	Related CSRs: 9.1.2, 9.3.1, 8.2.2, 9.5.1, 9.6.7, 9.6.8, 3.1.5	
<input type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		
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.	<ol style="list-style-type: none"> <li>1. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry".</li> <li>2. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.</li> </ol>	FISCAM
<p>Guidance: A good approach is to have needed data entry information succinctly formatted to facilitate ease of data entry.</p>	Related CSRs: 1.9.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
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.	<ol style="list-style-type: none"> <li>1. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<p>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.</p>	Related CSRs: 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 4.1.2, 4.1.3, 9.3.1, 9.3.6, 9.7.1	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		

**Category: Application System Accuracy Controls**

General Requirement Control Technique	Protocol	Reference
<p>9.6 Output production and distribution shall be controlled.</p> <p>9.6.1 Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review the documented procedure assigning responsibility for output production and distribution.</li> <li>2. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.</li> </ol>	FISCAM
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>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.</p> <p>Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation confirming use of the required process.</li> <li>3. Review documentation describing how the required control is implemented.</li> </ol>	FISCAM
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>9.6.3 The data processing control group, or some alternative, has a schedule by application that shows: (1) when outputs are completed; (2) when they need to be distributed; (3) who the recipients are; and (4) the copies needed. The group then reviews output products for general acceptability and reconciles control information to determine completeness of processing.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect the required schedule to confirm inclusion of the required elements.</li> <li>3. Inspect audit data confirming that the required process is consistently used.</li> </ol>	FISCAM
<p style="text-align: center;"> <input type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>9.6.4 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message.</p> <p>Guidance: The printed report name, time, and date are good management tools to assist in the tracking of completed tasks.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review sample printed reports to verify that it contains the elements required in the Control Technique.</li> </ol>	FISCAM
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>9.6.5 Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.</p> <p>Guidance: The output report log is a good management tool to assist in the tracking of completed tasks.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review logs and check sample output, to verify that the required information is recorded.</li> </ol>	FISCAM
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

**Category: Application System Accuracy Controls**

General Requirement Control Technique	Protocol	Reference
<p>9.6.6 Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.</p> <p>Guidance: The printed reports are good management tools to assist in the tracking of completed tasks. Related CSRs: 1.5.2</p>	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review the documented procedure describing the output process and supervisory review.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>9.6.7 A control log of output product errors is maintained, including the corrective actions taken.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review the control log and confirm that it contains the required information.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
<p>9.6.8 Output from reruns is subjected to the same quality review as the original output.</p> <p>Guidance: Data integrity is maintained by automating the output checks before the data is transmitted.</p>	<ol style="list-style-type: none"> <li>1. Inspect audit data confirming that the required process is consistently used.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
-----		
<p>9.7 Reports showing the results of processing shall be reviewed by users.</p> <p>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.</p> <p>Guidance: The user department has ultimate responsibility for maintaining data quality, and should review output reports for data accuracy, validity, and completeness.</p>	<ol style="list-style-type: none"> <li>1. Review the documented procedure describing the review process and detailed report constituency.</li> <li>2. Inspect audit data confirming that the required process is consistently used.</li> <li>3. Review sample reports to confirm that they include the required elements specified in the Control Technique.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		
-----		
<p>9.8 Programmed validation and edit checks shall identify erroneous data.</p> <p>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.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. Review the documented procedure describing the protection provided program code, files, or tables.</li> <li>2. Observe the actions or procedures in place that protect program code, files, or tables.</li> </ol>	FISCAM
<input checked="" type="checkbox"/> <i>SS</i> <input type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input type="checkbox"/> <i>CWF</i>		

**Category: Application System Accuracy Controls**

General Requirement	Control Technique	Protocol	Reference
9.8.2	<p>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.</p> <p>Guidance: Programmed validation and edit checks are, for the most part, the most critical and comprehensive set of controls in assuring that the initial recording of data into the system is accurate. For example, programmed validation and edit checks can effectively start as the data are being keyed in at a computer workstation using preformatted computer screens.</p>	<ol style="list-style-type: none"> <li>Review the documented procedure describing programmed validation and edits for inclusion of the specifically required checks.</li> <li>Inspect audit data confirming that the required process is consistently used.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 9.6.2, 3.4.1</p>
	<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		
9.8.3	<p>Validation and editing are performed at the computer workstation during data entry or are performed as early as possible in the data flow and before updating the master files. All data fields are checked for errors before rejecting a transaction.</p> <p>Guidance: Validation of the accuracy of data assists in the integrity of the data being processed.</p>	<ol style="list-style-type: none"> <li>Review the documented procedure describing the specified validation and editing process.</li> <li>Inspect audit data confirming that the required process is consistently used.</li> <li>Observe the validation and edit process.</li> </ol>	<p>FISCAM</p> <p>Related CSRs: 3.4.1</p>
	<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input type="checkbox"/> <i>CWF</i></p>		
9.9	<p>When appropriate, preformatted computer workstation screens shall be used for data entry.</p>		
9.9.1	<p>Preformatted computer workstations screens are utilized and allow prompting for data to be entered and editing of data as it is entered.</p> <p>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.</p>	<ol style="list-style-type: none"> <li>Review documented procedure specifying preformatted workstation screens, and describing screen prompts.</li> <li>Observe a sample of workstation screens as personnel are processing data.</li> <li>Interview the system administrator to confirm that the required feature is universally available..</li> </ol>	<p>FISCAM</p> <p>Related CSRs:</p>
	<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		

**10. Network**

10.1	<p>LAN/Computer Room Access Controls shall be in place.</p>		
10.1.1	<p>An access list of personnel authorized to access a data center to process sensitive data is controlled.</p> <p>Guidance: Ensure that only personnel with a need-to-know have access to the list.</p>	<ol style="list-style-type: none"> <li>By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center.</li> <li>Review audit data confirming control of access lists in accordance with documented procedures.</li> <li>Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	<p>CMS</p> <p>Related CSRs: 2.2.23</p>
	<p><input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i></p>		

Category: *Network*

General Requirement Control Technique	Protocol	Reference
10.1.2 Physical access to enclosures housing network equipment is restricted.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>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.</li> </ol>	CMS
<p>Guidance: Ensure that access to the area where the network equipment is located is controlled. Related CSRs:</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
10.2 Network system security shall be monitored for deficiencies.		
10.2.1 Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation identifying devices selected to provide the specified logging function.</li> <li>3. By inspection of a sample of the logs, confirm that they include network and system activity.</li> </ol>	CMS
<p>Guidance: Ensure that logs are kept of network activity. Related CSRs:</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
10.2.2 Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network.	<ol style="list-style-type: none"> <li>1. Confirm by inspection that virus-scanning software is installed.</li> <li>2. Confirm by inspection that virus-scanning software is installed.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>4. Review documentation identifying designated critical network entry points.</li> </ol>	CMS
<p>Guidance: A formal virus protection program should be established at the Network level. Related CSRs: 5.12.1</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		
10.2.3 Intrusion detection software is implemented providing real-time identification of unauthorized use, misuse, and abuse of computer assets by internal network users and external hackers.	<ol style="list-style-type: none"> <li>1. Review alarm and alert functions of any firewalls and other network perimeter access control systems to insure they are properly enabled.</li> <li>2. Review operating system, user accounting, and application software audit logging processes on all host and server systems to insure they are properly enabled.</li> <li>3. Review relevant policies and procedures for inclusion of the required process.</li> <li>4. Review sample of intrusion detection audit logs for servers and hosts on the internal, protected, network.</li> </ol>	CMS
<p>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</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>      <input checked="" type="checkbox"/> <i>PartB</i>      <input checked="" type="checkbox"/> <i>PartA</i>      <input checked="" type="checkbox"/> <i>Dmerc</i>      <input checked="" type="checkbox"/> <i>DC</i>      <input checked="" type="checkbox"/> <i>CWF</i> </p>		

Category: *Network*

General Requirement	Control Technique	Protocol	Reference
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.	<ol style="list-style-type: none"> <li>Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>Inspect logs confirming conduct of the required verification.</li> </ol>	CMS IRS 1075
Guidance:	A good approach might be a policy that requires verification of the receiving facsimile machine's telephone number.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>
	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
10.3.2	When sending or receiving sensitive fax information, have a trusted staff member at both sending and receiving fax machines, or have a locked room for the fax machine with custodial coverage over outgoing and incoming transmissions.	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS IRS 1075
Guidance:	a good approach might be a policy that states "If a locked room with custodial coverage is unavailable, trusted staff members are required to be at both the transmitting and receiving machines prior to transmittal."	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>
	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
10.3.3	Policy exists identifying appropriate use of the E-mail system by employees, and procedures exist to enforce E-mail security, privacy, and message integrity	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS
Guidance:	Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>
	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
10.3.4	Security policy exists and audit reviews include checks, to assure that system administrators and others with special system level access privileges are prohibited from reading the E-mail messages of others unless authorized on a case by case basis by appropriate management officials.	<ol style="list-style-type: none"> <li>Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>Inspect the audit process for operation in accordance with the documented process.</li> </ol>	CMS
Guidance:	Establish a policy to distribute procedures to all necessary personnel and develop a process to document the acknowledgement of the personnel. Ensure that policy exists and it contains the necessary checks with regards to audit reviews.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>
	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>
10.3.5	Fax procedures for sensitive information require a cover sheet that explicitly provides guidance to the recipient, which includes: (1) Notification of sensitive data and need for protection, and (2) Notice to unintended recipients to telephone the sender, collect if necessary, to report the disclosure and confirm destruction of the information.	Review relevant policies and procedures for inclusion and directed use of the required process.	CMS IRS 1075
Guidance:	Establish a formal procedure generating and attaching the required fax cover sheet.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i>	<input checked="" type="checkbox"/> <i>PartB</i>	<input checked="" type="checkbox"/> <i>PartA</i>
	<input checked="" type="checkbox"/> <i>Dmerc</i>	<input checked="" type="checkbox"/> <i>DC</i>	<input checked="" type="checkbox"/> <i>CWF</i>

Category: *Network*

General Requirement	Control Technique	Protocol	Reference
10.4 Cryptographic tools shall be controlled.			
10.4.1	Sensitive information being electronically transmitted must be protected. Two acceptable methods for transmitting sensitive information over telecommunications devices: (1) encryption and (2) guided media.	<ol style="list-style-type: none"> <li>1. Confirm by inspection that documented controls are in place and operational.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>3. Review documentation of controls used to assure protection of electronically transmitted sensitive information.</li> <li>4. Review documentation establishing approval of the protection methods utilized.</li> </ol>	FISCAM HIPAA IRS 1075
Guidance:	Ensure that a means of protecting sensitive information during transmittal has been implemented. Guided media is generally acceptable for internal transmissions within protected facilities. Encryption is typically required for transmission outside of protected facilities or through uncontrolled or public facilities or systems.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
10.4.2	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs when no other means of protection exists.	<ol style="list-style-type: none"> <li>1. Review documentation establishing that the required protection has been implemented.</li> <li>2. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM HIPAA
Guidance:	In some cases—especially those involving telecommunications—it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs, both while these data and programs are “in” the computer system and while they are being transmitted to another computer system or stored on removable media, such as floppy disks, which may be held in a remote location.	Related CSRs:	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
10.5 Adequate Network password policies shall be implemented.			
10.5.1	Passwords are transmitted and stored using secure protocols and algorithms.	<ol style="list-style-type: none"> <li>1. Review documentation of controls used to assure that all systems remain configured to use the specified feature.</li> <li>2. Review documentation explaining how this feature is implemented on each network and local computing environment.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> </ol>	FISCAM
Guidance:	Ensure that passwords are not transmitted as plain-text.	Related CSRs: 2.9.7, 10.10.1	
	<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

General Requirement Control Technique	Protocol	Reference
<p>10.6 Internet Security Policies shall be made available.</p> <p>10.6.1 CMS Business Partner's Internet connections must be in accordance with the CMS Internet Security Policy. When a determination for Internet use has been made, it shall include at a minimum of Triple 56-bit DES (defined as 112-bit equivalent) for symmetric encryption, 1024-bit algorithms for asymmetric systems, and 160-bit for the emerging Elliptical Curve systems (CMS Internet Security Policy, dated November 24, 1998).</p> <p>Guidance: At present, the internet may not be used for CMS sensitive data.</p>	<ol style="list-style-type: none"> <li>1. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement.</li> <li>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.</li> <li>3. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>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.</li> </ol>	CMS
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>10.7 Configuration Control Policy shall be documented and available.</p> <p>10.7.1 Purchased software is used in accordance with contract agreements and copyright laws</p> <p>Guidance: A formal policy should be established regarding the use of purchased software.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing audit and inventory processes and tools in use to detect improper use of software.</li> </ol>	CMS
<p style="text-align: center;">           Guidance: A formal policy should be established regarding the use of purchased software.      Related CSRs: 1.13.3  <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		
<p>10.7.2 Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software</p> <p>Guidance: A formal program should be established with a policy and procedure.</p>	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Confirm by inspection that the specified controls are in place and operating in accordance with the documented procedure.</li> <li>3. Review documentation describing the software tracking system implemented to provide the specified controls.</li> </ol>	CMS
<p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                <input checked="" type="checkbox"/> <i>PartB</i>                <input checked="" type="checkbox"/> <i>PartA</i>                <input checked="" type="checkbox"/> <i>Dmerc</i>                <input checked="" type="checkbox"/> <i>DC</i>                <input checked="" type="checkbox"/> <i>CWF</i> </p>		

General Requirement Control Technique	Protocol	Reference
10.7.3 A change-control mechanism that maintains control of changes to hardware, software, and security mechanisms is implemented.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review audit data confirming use of the documented change-control mechanism.</li> <li>3. Review documentation describing the change-control mechanism that is implemented to provide the specified controls..</li> <li>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.</li> <li>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.</li> </ol>	CMS
Guidance: A good approach might be to establish change control policies and procedures for all hardware, software, and security products.	Related CSRs: 5.9.3, 6.6.1, 3.4.1, 1.9.3, 6.1.2, 6.3.4	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
10.8 Logical Network Access Controls shall be in place.		
10.8.1 Any connection to the internet, or other external networks or systems, occurs through a gateway/firewall.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing controls implemented to insure compliance with this requirement.</li> </ol>	CMS FISCAM IRS 1075
Guidance: A firewall must separate corporate computers and servers from the internet or other external networks or systems. Workstations and servers behind the corporate firewall must not have a modem connection. Modem connections will be handled via an authorized dial-in server.	Related CSRs:	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		
10.8.2 Authentication is used to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; (3) grant access to the functions of critical network devices; (4) procedures for the above are documented.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Review documentation describing implementation of all required authentication functions.</li> </ol>	CMS HIPAA
Guidance: A formal program should be established with a policy and procedure.	Related CSRs: 2.9.6, 2.9.5	
<input checked="" type="checkbox"/> <i>SS</i> <input checked="" type="checkbox"/> <i>PartB</i> <input checked="" type="checkbox"/> <i>PartA</i> <input checked="" type="checkbox"/> <i>Dmerc</i> <input checked="" type="checkbox"/> <i>DC</i> <input checked="" type="checkbox"/> <i>CWF</i>		

General Requirement		Protocol	Reference
Control Technique			
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.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol>	FISCAM
	<p>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.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                          <input checked="" type="checkbox"/> <i>PartB</i>                          <input checked="" type="checkbox"/> <i>PartA</i>                          <input checked="" type="checkbox"/> <i>Dmerc</i>                          <input checked="" type="checkbox"/> <i>DC</i>                          <input checked="" type="checkbox"/> <i>CWF</i> </p>		Related CSRs: 2.8.7
10.8.4	Workstation with dial-up access generate a unique identifier code before connection is completed.	<ol style="list-style-type: none"> <li>1. Review documented dial-up procedure to confirm inclusion of the required features.</li> <li>2. Observe a sample of dial-up connections involving each type of access controller.</li> </ol>	FISCAM
	<p>Guidance: If workstations have dial-up access, ensure that a unique ID code is generated for each dial-up session.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                          <input checked="" type="checkbox"/> <i>PartB</i>                          <input checked="" type="checkbox"/> <i>PartA</i>                          <input checked="" type="checkbox"/> <i>Dmerc</i>                          <input checked="" type="checkbox"/> <i>DC</i>                          <input checked="" type="checkbox"/> <i>CWF</i> </p>		Related CSRs:
-----			
10.9	Vulnerabilities to physical and cyber attacks shall be assessed.		
10.9.1	A plan is in place to assess the risks to the network.	Review the required plan and approved implementing instructions.	PDD 63
	<p>Guidance: A formal program is in place for determining when and how to assess risks to the network.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                          <input checked="" type="checkbox"/> <i>PartB</i>                          <input checked="" type="checkbox"/> <i>PartA</i>                          <input checked="" type="checkbox"/> <i>Dmerc</i>                          <input checked="" type="checkbox"/> <i>DC</i>                          <input checked="" type="checkbox"/> <i>CWF</i> </p>		Related CSRs:
10.9.2	A plan is developed for eliminating significant vulnerabilities.	<ol style="list-style-type: none"> <li>1. Review the required plan.</li> <li>2. Review documentation establishing that the required plan eliminates all significant vulnerabilities.</li> </ol>	PDD 63
	<p>Guidance: As part of the security management program, ensure that a plan is developed to minimize vulnerabilities.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                          <input checked="" type="checkbox"/> <i>PartB</i>                          <input checked="" type="checkbox"/> <i>PartA</i>                          <input checked="" type="checkbox"/> <i>Dmerc</i>                          <input checked="" type="checkbox"/> <i>DC</i>                          <input checked="" type="checkbox"/> <i>CWF</i> </p>		Related CSRs:
10.9.3	A plan is developed for alerting, containing, and rebuffing a physical or cyber attack on the CMS Business Partner IS systems.	Review the required plan to confirm that it includes the specified features.	PDD 63
	<p>Guidance: A formal program should be established with documented policies and procedures.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                          <input checked="" type="checkbox"/> <i>PartB</i>                          <input checked="" type="checkbox"/> <i>PartA</i>                          <input checked="" type="checkbox"/> <i>Dmerc</i>                          <input checked="" type="checkbox"/> <i>DC</i>                          <input checked="" type="checkbox"/> <i>CWF</i> </p>		Related CSRs:
10.9.4	Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.	<ol style="list-style-type: none"> <li>1. Review relevant policies and procedures for inclusion and directed use of the required process.</li> <li>2. Inspect audit data confirming conduct of the required assessments at least annually.</li> </ol>	PDD 63
	<p>Guidance: As part of the security management program, ensure that an annual assessment is performed.</p> <p style="text-align: center;"> <input checked="" type="checkbox"/> <i>SS</i>                          <input checked="" type="checkbox"/> <i>PartB</i>                          <input checked="" type="checkbox"/> <i>PartA</i>                          <input checked="" type="checkbox"/> <i>Dmerc</i>                          <input checked="" type="checkbox"/> <i>DC</i>                          <input checked="" type="checkbox"/> <i>CWF</i> </p>		Related CSRs: 1.9.8

Category: *Network*

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 IDs and passwords for access to specific applications; (2) control access through connections between systems and workstations; (3) restrict an application's use of network facilities; (4) protect sensitive data during transmission; (5) automatically disconnect at the end of a session; (6) maintain network activity logs; (7) restrict access to table that define network options, resources, and operator profiles; (8) allow only authorized users to shutdown network components; (9) monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; (10) restrict in-house access to telecommunications software; (11) control changes to telecommunications software; (12) ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage and; (13) restrict and monitor access to telecommunications hardware or facilities.	1. Review documentation confirming implementation of communications software having all of the required features. 2. Review audit data confirming continuing operation of all specified features of the required software.	FISCAM
Guidance: Ensure that policies and procedures are in place that address all thirteen (13) of these points. If not, they should be developed in coordination with you company's IT department.	Related CSRs: 6.4.1, 2.9.6, 2.9.11, 2.8.4, 3.4.1, 2.9.8, 2.9.10, 3.6.2, 10.5.1	
✓ SS	✓ PartB	✓ PartA
✓ Dmerc	✓ DC	✓ CWF