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

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

(Rev. 7, 03-17-06)

CMS/Business Partners
Systems Security Manual

Table of Contents
(Rev. 6, 12-09-05)

Appendices

1.0 - Introduction

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, fiscal intermediaries, Common Working File (CWF) host sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, regional laboratory carriers, claims processing data centers, Medicare Administrative Contractors (MACs) and Enterprise Data Centers (EDCs).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). In this manual the terms “business partner” and “contractor” are used interchangeably, and all provisions that apply to business partners also apply to MAC contractors.

This manual addresses the following key business partner security elements:

- An overview of primary roles and responsibilities

- A program management planning table that will assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites

- Appendix A: The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs), which provides the following:

The CSRs http://www.cms.hhs.gov/manuals/downloads/117_systems_security_AtchA.pdf
An overview of the CISS data collection and reporting process.
The CMS IT systems security program and CSRs were developed in accordance with Federal and CMS documents that mandate the handling and processing of Medicare data. These documents include the following:

- CMS System Security Plans (SSP) Methodology, Draft Version 3.0, November 6, 2002

- http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf

- Federal Information Security Management Act of 2002 (FISMA), November 27, 2002

- http://csrc.nist.gov/policies/FISMA-final.pdf

- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996

- http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

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

- http://www.gao.gov/special.pubs/ai12.19.6.pdf

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, June 2000

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

- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (PUBLIC LAW 108–173), DEC. 8, 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors

- http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf

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

- http://www.whitehouse.gov/omb/circulars/a127/a127.html
- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999
- http://www.whitehouse.gov/omb/circulars/index.html
- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000
- http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- **Appendix III to** OMB **Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000**
- http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html
- Presidential Decision Directive/NSC – 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998
- http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
- Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to provider of service
- http://www.ssa.gov/OP_Home/ssact/title18/1816.htm
- Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits
- http://www.ssa.gov/OP_Home/ssact/title18/1842.htm
- Public Law 93-579, The Privacy Act of 1974, as amended
- http://www.supremelaw.org/ref/pl93-579/pl93-579.htm
- Public Law 99-474, Computer Fraud & Abuse Act of 1986
- http://nsi.org/Library/Compsec/cfa.txt
- Public Law 100-235, Computer Security Act of 1987
- http://www.nist.gov/cfo/legislation/Public Law 100-235.pdf
- Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35
- http://www.estrategy.gov/documents/16.pdf

- Public Law 104-106, Clinger-Cohen Act of 1996 (formerly called the Information Technology Management Reform Act)

- http://www.mfrc-dodqol.org/pdffiles/childcare_act.pdf

- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA), 1996

- http://aspe.os.dhhs.gov/admnsimp/index.shtml

- Public Law 106-398, National Defense Authorization Fiscal Year 2001, Government Information Security Reform Act (GISRA) of 2000

- http://peoammo.army.mil/PEOAMMO/CIO Web/CIO References/US Code Extracts/PL 106-398 Sec 811.doc

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

- CMS Information Security Acceptable Risk Safeguards (ARS) Version 1.2, October 25, 2004

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

- CMS Information Security Certification and Accreditation (C&A) Methodology, Version 1.0, May 12, 2005

- http://cms.hhs.gov/it/security/docs/C&A_meth.pdf

- CMS Information Security Risk Assessment (RA) Methodology, Version #2.1 April 22, 2005

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

- CMS Information Security Risk Assessment (RA) and System Security Plan (SSP) Guidance, Version # 1.0 September 3, 2004

- http://cms.hhs.gov/it/security/docs/RA_and_SSP_guidance.pdf

- Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731

- http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html

- United States Code Title 44 Chapter 33—Disposal of Records

- http://www4.law.cornell.edu/uscode/html/uscode44/usc_sup_01_44_10_33.html

- Department of Health and Human Services (DHHS), IRM Policies and Guidelines

- http://www.hhs.gov/read/irmpolicy/index.html
- Federal Information Processing Standards Publications (FIPS) PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25 U.S. Department of Commerce/National Institute of Standards and Technology (NIST), PUB46-3
- http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- Homeland Security Presidential Directive/HSPD-7
- http://www.fas.org/irp/offdocs/nspd/hspd-7.html
- National Institute of Standards and Technology SP 800-26, Security Self Assessment Guide for Information Technology Systems, November 2001
- http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, SP800-12
- http://csrc.nist.gov/publications/nistpubs/800-12
- NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide, January 2004
- http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004
- http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html.
- CMS Policy for the Information Security Program, May 2005
- http://cms.hhs.gov/it/security/docs/policy_is_program.pdf

1.1 - Additional Requirements for MAC Contractors

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

MAC contractors are responsible for fulfilling all existing business partner requirements. Further, additional requirements are specified in Section 912 of the Medicare Modernization Act (MMA). These additional requirements include the following:

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 calendar days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.
- The contractor shall comply with the CMS Certification and Accreditation (C&A) methodology, policies, standards, procedures, and guidelines for contractor

facilities and systems. The CMS C&A methodology can be found on the CMS web site http://www.cms.hhs.gov/it/security.

- The contractor shall conduct or undergo an independent evaluation and test of its systems security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under the contract.

- The contractor shall support CMS validation and accreditation of contractor systems and facilities in accordance with CMS C&A methodology.

- The contractor shall provide annual certification, in accordance with C & A methodology, that they have examined the management, operational, and technical controls for its systems supporting the MAC function, and consider these controls adequate to meet CMS security standards and requirements.

The contractor shall appoint a Chief Information Officer to oversee its compliance with the CMS security requirements. The contractor's SSO shall be a full-time position dedicated to assisting the CIO in fulfilling the requirements.

2.0 - IT Systems Security Roles and Responsibilities

(Rev. 3, 03-28-03)

2.1 - Consortium Contractor Management Officer and CMS Project Officer (CCMO/PO)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The Consortium consists of four offices (Northeastern, Southern, Midwestern, and Western). The CCMO is a part of the Consortium and is responsible for CMS contract management activities. CCMOs are responsible for the oversight of Medicare carriers and fiscal intermediaries. CMS POs (generally located in Central Office business components) oversee the other business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The CCMO/PO has the following responsibilities:

- CMS point of contact for business partner IT systems security problems

- Central point for the reception of IT SSPs and reports including security incident reports

- Provider of technical assistance necessary to respond to CMS security policies and procedures.

2.2 - The (Principal) Systems Security Officer (SSO)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Business partners must designate an SSO qualified to manage the Medicare system security program and ensure the implementation of necessary safeguards.

The SSO must be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development. A qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization. A sound entity-wide security program is the cornerstone of effective security control implementation and

maintenance. The SSO position for each contractor should be full-time and fully qualified—and preferably credentialed in systems security. Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available Line One funding.

A business partner may have additional SSOs at various organizational levels, but it must coordinate security actions through the principal SSO for Medicare records and operations. The SSO ensures compliance with CMS CSRs by:

- Facilitating the Medicare IT system security program and ensuring that necessary safeguards are in place and working
- Coordinating system security activities throughout the organization
- Ensuring that IT systems security requirements are considered during budget development and execution
- Reviewing compliance of all components with the CMS CSRs and reporting vulnerabilities to management
- Establishing an incident response capability, investigating systems security breaches, and reporting significant problems (see section 3.6) to business partner management and CMS
- Ensuring that technical and operational security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes
- Ensuring that IT systems security requirements are included in Request For Proposals (RFPs) and subcontracts involving the handling, processing, and analysis of Medicare data
- Maintaining systems security documentation in the System Security Profile for review by CMS and external auditors
- Cooperating in all official external evaluations of the business partner's systems security program
- Facilitating the completion of the Risk Assessment (see section 3.2)
- Ensuring that an operational IT Systems Contingency Plan is in place and tested (see section 3.4)
- Documenting and updating the monthly Plan of Action and Milestones (POA&M—see section 3.5.2). Updates may occur whenever a POA&M projected

completion date passes, and following the issuance of new requirements, risk assessments, internal audits, and external evaluations (The schedule and updates are highly sensitive and should have limited distribution).

- Keeping all elements of the business partner's System Security Profile secure (see section 3.7)

- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix B).

The Principal SSO should earn 40 hours of continuing professional education credits each year from a recognized national information systems security organization. The educational sessions at the security best practices conference can be used towards fulfilling CMS business partners' continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the best practices conference agenda.

2.3 - System Owners/Managers

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Business partner System Owners/Managers are responsible for:

- Determining and documenting the data sensitivity and application criticality of the resources for which they are responsible

Identifying appropriate security level designations for their systems.

2.4 - System Maintainers/Developers (Rev. 3, 03-28-03)

Business partner System Maintainers/Developers have the responsibility to implement the security requirements throughout the System Development Life Cycle (SDLC) using the security level designation as the basis.

2.5 - Personnel Security/Suitability

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

All business partner and contractor employees requiring access to CMS sensitive information must meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum: contacting references provided by the employee and contacting the local law enforcement agency or agencies.

3.0 - IT Systems Security Program Management

(Rev.6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Business partners must have policies and procedures, and implement controls or plans that fulfill the CMS CSRs (see Attachment A).

Policies are formal, up-to-date, documented rules stated as "shall" or "will" statements that exist and are readily available to employees. They establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up-to-date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Controls are measures implemented to protect the confidentiality, integrity, and availability of sensitive information. IT security procedures and controls shall be implemented in a consistent manner everywhere that the procedure applies. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that controls are operating as intended.

Note that meeting requirements does not validate the quality of a program. Managers with oversight responsibility must understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and provides high-level descriptions for them. As appropriate, this section refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners must perform a Self-Assessment using the CMS CSRs. The weaknesses, action plans, and POA&Ms must be recorded in the CISS (See Appendix A). To perform the Self-Assessment, business partners must conduct a systematic review of the CSRs using the CISS. The CISS provides a Self-Assessment form that includes guidance and audit protocols to assist in the review of the requirements.

The CMS CSRs include key security-related tasks. Table 3.1 indicates how often these tasks need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a “do by” date. The number accompanying each entry in the requirement column indicates the section in this document that deals with the particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Table 3.1. Reporting Requirements Planning Table

Requirement	Frequency	Send To	Comments	Complete (check when complete)
Appendix A, Self-Assessment using the CISS	Each Federal FY	CCMO/PO with a copy to CMS CO System Security Profile	See Appendix A for an overview of the CISS. Self-Assessment results recorded using the CISS are to be discussed in the Certification Package.	☐
3.1 System Security Plans	The SSP for each General Support System & Major Application must be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change[1].	System Security Profile SSO CMS CO	SSPs are to be reviewed, updated, and certified by management—and indicated as such in both the Certification Package/statement of certification and the System Security Profile.[2]	☐
3.2 Risk Assessment (Report)	The Risk Assessment for each GSS and MA must be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change[1].	System Security Profile CMS CO	Risk Assessments are to be reviewed, updated, and certified by management—and indicated as such in both the Certification Package/statement of certification and the System Security Profile. The Risk Assessment Report is an attachment to the System Security Plan.[3]	☐
3.3 Certification	Each Federal FY	CCMO/PO with a copy to CMS CO System Security Profile	Fiscal intermediaries and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-6) information on certification requirements including where, when, and to whom these certifications must be submitted. All other contractors should submit a statement of security certification to their CMS POs.	☐
3.4 IT Systems Contingency Plan	Contingency Plans must be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change[4]. Plans must be tested annually.	System Security Profile SSO CMS CO	Management and the SSO must approve the Plan. The IT Contingency Plan is to be developed (in accordance with Appendix B), reviewed, updated, and certified by management—and indicated as such in both the Certification Package/statement of certification and the System Security Profile.[5]	☐

[1] *NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."*

[2] *More information about system security planning can be found in the CMS SSP Methodology.*

[3] *More information about Risk Assessment Reports can be found in the CMS Information Security Risk Assessment (RA) Methodology.*

[4] *NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."*

[5] *More information about contingency planning can be found in An Introduction to Computer Security: The NIST Handbook. SP 800-12, and the Contingency Planning Guide for Information Technology Systems: NIST Special Pub 800-34.*

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.5 Compliance	Each Federal FY	CCMO/PO System Security Profile SSO CMS CO	There are two (2) components to compliance: (1) ACA: Once a year, an independent audit will be performed on four (4) categories of the CMS CSRs to validate the Self-Assessment. CMS will determine the four categories the audit will validate and inform the business partners via the BPSSM. (2) POA&Ms: POA&Ms address findings of annual system security assessments including the ACA, the annual CMS Self Assessment Review, and, as applicable: SAS 70 audits, CFO controls audits, the Section 912 evaluation, and data center tests and reviews.	☐ ☐
3.6 Incident Reporting and Response	As necessary	CCMO/PO System Security Profile	The HIPAA also addresses Incident Reporting information.	☐
3.7 System Security Profile	As necessary	On file with the Security Organization		☐

LEGEND:

ACA	Annual Compliance Audit
CCMO	Consortium Contractor Management Officer
CFO	Chief Financial Officer
CISS	CMS Integrated Security Suite
CO	Central Office (CMS)
CPIC	Certification Package for Internal Controls
FY	Fiscal Year
GSS	General Support System
MA	Major Application
PO	Project Officer (CMS)
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer

Note: Documents listed in table 3.1 may be stored as paper documents, electronic documents, or a combination thereof.

When submitting documentation to CCMOs or to the CMS Central Office, use Federal Express, certified mail, or the equivalent (receipt required). For supporting documentation (such as Risk Assessments, Contingency Plans, System Security Plans, etc.), only digital soft copies in the approved CMS format are required. Paper copies are only required for certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:

- **CMS Central Office**

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

Following are the contacts and addresses for the four Consortia:

- **Northeast Consortium**

Consortium Contractor Management Officer
Philadelphia Regional Office, Suite 216

The Public Ledger Building
150 S. Independence Mall West
Philadelphia, PA 19106
215-861-4191

- **Southern Consortium**

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

- **Midwest Consortium**

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

- **Western Consortium**

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

3.1 - System Security Plan (SSP)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The objective of an information security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process or store Medicare-related data have some level of sensitivity and require protection. The protection of a system must be documented in an SSP. The completion of an SSP is a requirement of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either a Major Application (MA)[6] or General Support System (GSS)[7] must be covered by SSPs.

---

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

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

The purpose of an SSP is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager (i.e., SSO).

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

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

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

SSPs must be re-certified within 365 days from the last date certified. The SSP must also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update to the SSP needs to occur. The SSP must be updated if there has been a significant change[8] or the security posture has changed. Examples of significant change[8] include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review must be placed in the Medicare contractor's System Security Profile. The updated SSP must be placed in the Medicare contractor's System Security Profile and a copy must be provided to the CMS Central Office.

Contractors given direction to update their current SSP(s) to include front-end, back-end, and/or other claims processing systems must use the most current version of the CMS System Security Plan Methodology. The CMS methodology and template can be found on the CMS website at http://www.cms.hhs.gov/it/security/References/ps.asp. Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These

---

[8] *NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."*

front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions. Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc). These back-end systems include, but are not limited to: print mail, 1099, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

A newly developed or updated SSP including the original signed, dated CMS SSP certification form must be sent to the CMS Central Office. These documents must be received by CMS on CD-ROM ten (10) working days after they have been developed, updated, or re-certified, and the original signed, dated CMS SSP certification form (Tab A, Appendix A of the CMS SSP Template) must be submitted in hard copy along with the electronic copy. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

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

Should SSP technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-620-8585.

3.2 - Risk Assessment

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Business partners are **required** to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology and the CMS Information Security RA and SSP Guidance. These documents are available at:
http://www.cms.hhs.gov/it/security/References/ps.asp.

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

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

All RAs must be re-certified within 365 days from the last date certified. Medicare contractors must review their RA(s) prior to re-certification to determine if an update is needed. An RA must be performed if a significant change[9] to any information system has occurred. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security

[9] *NIST* defines "significant change" *as* "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."

posture. Documentation of the review and/or the updated RA must be placed in the Medicare contractor's System Security Profile. The updated RA(s) must also be mailed to the CMS Central Office. The RA used to support a SSP(s) cannot be dated more than 12 months earlier than the SSP certification date.

Contractors that must update their current RA(s) must use the most current version of the CMS Information Security RA Methodology. The CMS methodology and template can be found on the CMS Web site at http://www.cms.hhs.gov/it/security/References/ps.asp.

A newly developed or updated RA that is an attachment to the SSP must be sent to the CMS Central Office. These documents must be received by CMS on CD-ROM ten (10) working days after they have been developed and updated. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

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

Should RA technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-620-8585.

Business partners should refer to the CMS Information Security Acceptable Risk Safeguards (ARS) document to aid in the preparation of a risk assessment. This document can be found at http://www.cms.hhs.gov/it/security/References/ps.asp.

3.3 - Certification

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

Each contractor is required to self-certify to CMS its IT systems security compliance within each Federal fiscal year. This security certification will be included in the Certification Package for Internal Controls (CPIC) or, for contracts not required to submit CPIC certifications, send the security certification to their appropriate CMS POs. CMS will continue to require annual, formal re-certification within each fiscal year no later than September 30, including validation at all levels of security as described in this manual.

Systems security certification must be fully documented and maintained in official records. The Certification validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification
- Self-Assessment (see Appendix A)
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.4 and Appendix B)

- Results of the ACA (see section 3.5.1)
- Plan of Action and Milestones (see section 3.5.2).

3.4 - Information Technology Systems Contingency Plan

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

Appendix B to this manual provides information on Medicare IT Systems Contingency Plans. See Item 3.4 in Table 3.1, section 3.0, for other references.

Each Medicare contractor must review its IT Systems Contingency Plan 365 days from the date it was last reviewed or updated to determine if changes to the contingency plan are needed. A contingency plan should be updated if a significant change[10] has occurred. The system contingency plan must also be tested 365 days from the last test performed. Updated plans and test reports (results) should be placed in the contractor's System Security Profile. Business partner management and the SSO must approve newly developed or updated IT Systems Contingency Plans. Information on Medicare IT systems contingency planning can be found in Appendix B.

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

3.5 - Compliance

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Compliance refers to the contractual obligations of business partners to CMS. There are two components to electronic data processing (EDP) security reporting compliance: the ACA, and the Plan of Action and Milestones. Each is described in detail in the following subsections. All compliance-related reporting requirements are explained in the subsections that follow.

3.5.1 - Annual Compliance Audit (ACA)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

---

[10] *NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."*

Each business partner must conduct an Annual Compliance Audit (ACA) on four (4) out of the ten (10) categories of the CMS CSRs. See Appendix A, section 1.0 for a description of these 10 categories. A compliance audit is a performance review of a business partner's systems security program that tests whether the systems security controls comply with CMS' CSRs (Attachment A) and are implemented properly. The compliance audit is documented through an ACA Report. Government auditing standards dictate that business partner staff assigned to conduct an audit should possess adequate professional proficiency for the tasks required[11]. An audit team should possess audit skills and familiarity with implementation of the physical and IT security features utilized by the business partner or required by CMS. Required audit skills include proficiency in basic auditing tasks, communication skills, and project management skills. An internal audit department with these qualifications may perform an ACA.

An ACA will have a verifiable information system security auditor assigned to coordinate the interviews, tests, and analysis, and provide approval of the final report. The information systems auditor must not be part of the organization directly responsible for design, operation, and/or management of the systems being audited.

The ACA report must include the following:

1. A Summary of Controls. Refers to controls implemented by the business partner to comply with the CMS CSRs. The summary of controls should be derived from the source documentation referenced in the CMS Integrated Security Suite (CISS, formerly the Contractor Assessment Security Tool, a.k.a. "CAST").
2. A Description of Review Procedures and Tests. Must include procedures and tests performed by the organization (either internal or external) conducting the ACA, and a description of the results of such tests.

A CMS-directed SAS 70 and/or Office of Inspector General (OIG) Chief Financial Officer (CFO) EDP audit will meet the requirement of the identified CSR categories for the ACA if either audit was performed during the current fiscal year and addressed the categories identified by CMS for the current fiscal year. An ACA must be performed for those categories not covered by a SAS 70 or OIG CFO EDP audit.

The ACA must be completed by September 30, 2006. The CSR categories to be audited in FY2006 are: (1) Access control, (2) Application software development and change control, (3) Service Continuity, and (4) Network.

Medicare contractors who received Section 912 evaluations or data center system tests and evaluations in FY2005 or FY2006 do not need to conduct an ACA for FY2006. Those entities who are notified of gaps, weaknesses, and/or findings should focus on remediation of the identified issues in lieu of conducting an ACA. All Medicare contractors who did not receive Section 912 evaluations or data center system tests and evaluations must conduct an ACA.

A copy of the completed ACA must be submitted on CD-ROM to the CMS Central Office, the business partner's CCMO for Title XVIII contracts, or the PO for FAR contracts by October 13, 2006. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used. A copy must also be placed in the System Security Profile.

CMS recommends that the ACA report be organized by subject matter to facilitate ease of review and use. Report categories should include (1) CSR categories, (2) OIG CFO EDP audit,

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

(3) SAS 70 review, and/or (4) any other open findings from independent or external audits or reviews.

3.5.2 - Plan of Action and Milestones (POA&Ms)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Business partners are required to submit a monthly POA&M package consisting of several components. Among these components is a CISS-generated data file. The package also includes a hard copy of the CMS POA&M Weakness Tracking Form (the POA&M Excel spreadsheet), a CISS-generated report, documentation to support closed findings (if applicable), and other documentation as required by CMS.

3.5.2.1 - Background

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The Federal Information Security Management Act of 2002 (FISMA) requires that Federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency[12]. Additionally, periodic POA&Ms, reporting the status of known security weaknesses for all Federal agency systems, must also be submitted to the Office of Management and Budget (OMB)[13]. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under The Federal Managers Financial Integrity Act of 1982). In the case of FISMA, any security weakness[14] identified for covered systems must be reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of Business Partner Security Programs to ensure that they meet the information security requirements imposed by FISMA. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The CISS enables contractors to satisfy reporting requirements for EDP findings. Finding (and approved action plan) data is entered into the tool following all audits/reviews, from which CISS generates a single monthly submission data file that summarizes the state of security for the business partner. This data file is submitted to CMS as part of the monthly POA&M package.

3.5.2.2 - POA&M Package Components/Submission Format

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

---

[12] FISMA Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a Contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires that each agency provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, Contractor, or other source."

[13] POA&M instructions for Federal agencies are described in OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act.

[14] Weaknesses are defined as those vulnerabilities that require corrective action (CMS Plan of Action and Milestones (POA&M) Guide – June 22, 2004 – 2nd Draft)

In addition to the initial POA&M reporting that follows each audit/review, effective July 15, 2005, summary POA&Ms shall be submitted on the 15th of each month via the CISS. The CISS shall be populated with EDP findings from the Chief Financial Officer's Electronic Data Processing (CFO EDP) Audit, the Section 912 evaluation, data center security tests and evaluations, the SAS 70 review, the Certification Package of Internal Controls (CPIC), and any other EDP findings that result from an audit or review, whether internal or external. Corrective actions are to be established in the CISS to address all resulting weaknesses entered therein, and those corrective actions will be reflected in the CISS POA&M (both in the data file and reports). Additionally, the CISS data file, a hard copy of the CMS POA&M Weakness Tracking Form (the POA&M Excel Spreadsheet), and the CISS-generated report will be submitted simultaneously.

To ensure consistency, all Medicare contractors must enter into the CISS the Section 912 evaluation, Data Center System Test &Evaluation, and/or CFO EDP Audit POA&Ms that have already been accepted and approved by OIS for its EDP findings, as the standard for all future submitted POA&Ms. Findings from other audits, reviews and evaluations (e.g., SAS 70, CPIC, internal audits, etc.) that address the same problem should use the same solution (action plan) if it will adequately resolve the identified weakness.

Initial Report. Within 45 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review (with the exception of the ACA, which is due within 10 days), an initial, manually updated, CMS POA&M Weakness Tracking Form is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation. Upon acceptance from CMS, this information will be entered into the CISS by the Medicare contractor for monthly tracking purposes. Note: Medicare contractors are encouraged to use the draft reports (when available) to prepare their corrective actions for identified findings.

Monthly POA&M Package. On a monthly basis, business partners shall provide updates on progress towards completion of remediation efforts for weaknesses identified from all known sources. Due by the 15th, the monthly POA&M package will include:

CD-ROM. The CD should contain the CISS-generated data file (refer to the POA&M submission instructions in the CISS User Guide) at the root level, along with the CISS-generated POA&M report (exported to Excel), the electronic CMS POA&M Weakness Tracking Form (which contains the Section 912, Data Center ST&E, and/or CFO EDP findings), and documentation to support those findings (if applicable).

Documentation to support findings closed during a reporting cycle should be organized into separate folders, each named according to the finding number to which it pertains. The CD is to be labeled with the company name, the words "POA&M Data and Finding Closure Documentation," and the month and year of submission.

Hard copy documentation. In addition to the CD-ROM, the monthly POA&M package will include hard copies of:

- The CISS-generated summary POA&M report
- The CMS POA&M Weakness Tracking Form (the POA&M Excel spreadsheet), which contains the Section 912, Data Center ST&E, and/or CFO EDP audit findings.

Medicare contractors must submit the monthly POA&M package to the CMS Central Office and their CCMO (for Title XVIII and MAC contracts) or PO (for FAR contracts). Please be advised

that this information should not be submitted via email. Registered mail or its equivalent should be used. A copy must also be placed in the System Security Profile.

3.6 - Incident Reporting and Response

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

An incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The business partner must use its security policy and procedures to determine whether the security incident is reportable (as defined below). Upon receiving notification of an IT systems security incident or a suspected incident, the SSO will immediately perform an analysis to determine if an incident actually occurred. The incident could result in adversely impacting the processing of Medicare data or the privacy of Medicare data. Reportable incidents include:

- Unauthorized Disclosure: information disclosure with risk to privacy information or public relations impact
- Denial of Service: an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Malicious Code: a virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- Unauthorized Access: a breach in which person gains logical or physical access to network, system application, data or other resource without permission
- Inappropriate Usage: a violation of acceptable computing use policies

Multiple Component: a single incident that encompasses two or more incidents.

3.6.1 - Computer Security Incident Response

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

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

As part of the risk management process, the business partner should determine the extent of the incident's impact and the potential for new or enhanced controls required to mitigate newly identified threats. These new security controls (and associated threats and impacts) should

provide additional input into the business partner's risk assessment. Business partners shall refer to The CMS System Security Incident Handling Procedures for further guidance. This document can be found at http://www.cms.hhs.gov/it/security/References/ps.asp.

3.7 - System Security Profile

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Risk Assessments
- Completed CISS Self Assessments
- ACA Reports
- IT Systems Contingency Plans
- Security reviews undertaken by DHHS OIG, CMS, IRS, GAO, consultants, subcontractors, and business partner security staff
- POA&Ms for each security review
- System Security Plan (for each GSS and MA)
- Systems security policies and procedures
- Certifications (including, but not limited to systems security plan, risk assessment, and contingency plan certifications).

Secure the profile, keep it up-to-date, and maintain pointers to other relevant documents. Require secure off-site storage of a backup copy of the System Security Profile preferably at the site where back-up tapes and/or back-up facilities are located. Keep this back-up copy of the profile up-to-date, particularly the contingency plan report.

3.8 - Fraud Control

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Business partners are required to safeguard systems against fraud. The CMS CSRs address fraud control issues such as personnel screening, separation of duties, rotation of duties, and training. Business partners should practice fraud control in accordance with Appendix A, The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs), and Appendix C, An Approach to Fraud Control.

3.9 - Patch Management

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Timely patching is critical to maintaining the operational availability, confidentiality, and integrity of Medicare systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches. CERT/Coordination Center (CC) (http://www.cert.org) estimates that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches.

To help address this growing problem, CMS recommends that business partners have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. The CSRs provide specific guidance on time frames for implementation of patches.

NIST SP 800-40, Procedures for Handling Security Patches, provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS does not normally require the verbatim use of NIST publications for the configuration of Medicare systems. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop configuration standards, templates, and management processes that securely configure Medicare systems as part of their configuration management program.

3.10 - Security Management Resources

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

3.10.1 - Security Configuration Management

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government.

The guidelines and checklists are developed to help system operators configure security within these systems to the highest level possible. NIST provides these and other guidelines and checklists at http://csrc.nist.gov/pcig/cig.html.

The National Security Agency (NSA) has also developed and distributed configuration guidance for a wide variety of software from open-source to proprietary. The objective of the NSA configuration guidance program is to provide administrators with the best possible security options in the most widely used products. NSA provides these guidelines at http://www.nsa.gov/snac/downloads_all.cfm.

The Center for Internet Security (CIS) provides security configuration benchmarks that represent a prudent level of due care, and are working to define consensus best-practice security configurations for computers connected to the Internet. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks. The CIS benchmarks and scoring tools are available for download at http://www.cisecurity.com/benchmarks.html.

CMS does not require the verbatim use of these documents and tools for the configuration of Medicare systems. However, CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity. CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

NOTE: MACs and EDCs are required to start with these baseline configurations (Security Technical Implementation Guides (STIGs)) and then document any exceptions based on environment specific implementation.

The use of STIGs will:

- Reduce the likelihood of successful intrusions or attacks;
- Facilitate secure configuration of systems prior to network deployment; and

- Assist with monitoring systems for on-going conformance with security configurations.

Table 3.2 contains links to security configuration guidelines and checklists for some of the more common systems utilized within the Medicare business partner community. Table 3.2 is not meant to be all-inclusive and may contain some references that are not applicable to a particular Medicare business partner application. However, CMS highly encourages business partners to review and incorporate these concepts into the Medicare configuration management philosophy within their systems management and security programs.

Table 3.2. Configuration Guidelines

System Type	Standards and Checklists Available	Comments
Databases		
Oracle	1. http://www.oracle.com/technology/deploy/security/index.html	1. Oracle's Web site for security in Oracle products.
	2. http://www.cisecurity.com/bench_oracle.html	2. CIS site for system vulnerability assessment and configuration guidelines. Includes technical information on Oracle security configurations.
	3. http://csrc.nist.gov/pcig/STIGs/DATABASE-STIG-V7R1.pdf	3. DISA Database STIG.
	4. http://csrc.nist.gov/pcig/CHECKLISTS/db-checklist-v7r1-0-04212005.zip	4. DISA Database Security Checklist.
	5. http://www.nsa.gov/snac/downloads_all.cfm	5. NSA guidelines for Oracle security developed by NSA's Systems and Network Attack Center (SNAC).
	6. http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	6. DISA UNIX configuration guidelines. Contains information for general UNIX security and specifications for HP-UX.
Mainframe Security		
Unisys	1. http://csrc.nist.gov/pcig/CHECKLISTS/unisys_checklist_v612_121203.zip	1. DISA Unisys Security Readiness Review Checklist.
	2. http://csrc.nist.gov/pcig/STIGs/unisys-stig-v7r1.pdf	2. DISA Unisys STIG.
VMS	http://csrc.nist.gov/pcig/CHECKLISTS/vms-openvms_srrchklst_v2r2-01jan2005.zip	DISA VMS - OpenVMS VAX/ALPHA Security Readiness Review Security Checklist.
Networks		
General	1. http://csrc.nist.gov/pcig/CHECKLISTS/network-checklist-v5r2_4-042005.doc	1. DISA Network Infrastructure Security Checklist.

System Type	Standards and Checklists Available	Comments
	2. http://csrc.nist.gov/pcig/STIGs/NETWORK-STIG-V5R2%209-29-2003FINAL.doc	2. DISA Network Infrastructure STIG.
Novell	1. http://www.novell.com 2. http://support.novell.com/techcenter/articles/ana20000603.html 3. http://support.novell.com/techcenter/articles/ana19971104.html	1-3. Novell Web site. The developer.novell.com site contains white papers and technical guidelines for security in Novell products.
	4. http://novell.unc.edu/security/security.htm	4. University of North Carolina security guideline.
Operating Systems		
Macintosh	1. http://csrc.nist.gov/pcig/STIGs/MAC-OS-X-STIG-V1R1.pdf	1. DISA Macintosh OS-X STIG.
	2. http://csrc.nist.gov/pcig/CHECKLISTS/macosxchecklistv1r11.zip	2. DISA Macintosh OS-X Checklist.
OS/390 and MVS	1. http://csrc.nist.gov/pcig/STIGs/OS390LPAR-STIG-v2r2-Mar05.pdf	2. DISA OS/390 Logical Partition STIG.
	2. http://csrc.nist.gov/pcig/CHECKLISTS/lpar-checklist-2v103-062504.doc	3. DISA OS/390 Logical Partition Checklist.
	3. http://csrc.nist.gov/pcig/CHECKLISTS/racf-checklist-v4r14.doc	4. DISA OS/390 RACF Checklist.
	4. http://csrc.nist.gov/pcig/CHECKLISTS/acf2-checklist-v4r14.doc	5. DISA OS/390 ACF2 Checklist.
	5. http://csrc.nist.gov/pcig/CHECKLISTS/tss-checklist-v4r14.doc	6. DISA OS/390 TSS Checklist.
UNIX / AIX	1. http://publib-b.boulder.ibm.com/redbooks.nsf/redbookabstracts/sg246066.html?open	1. IBM Redbooks on AIX Security.
	2. http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	2. DISA UNIX configuration guidelines. Contains information for general UNIX security and specifications for AIX.
UNIX / HP-UX	http://www.cisecurity.com/bench_hpux.html	CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
UNIX / LINUX	1. http://www.cisecurity.com/bench_linux.html	1. CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.

System Type	Standards and Checklists Available	Comments
	2. http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	2. DISA UNIX configuration guidelines. Contains information for general UNIX security and specifications for LINUX.
	3. http://www.nsa.gov/selinux/index.html	3. NSA's Information Assurance Research Group developed guidelines and tools to implement LINUX for use in an environment with security requirements.
UNIX / Solaris	1. http://www.sun.com/solutions/blueprints/	1. Sun site for white papers (blueprints) on security and other Solaris topics.
	2. http://sunsolve.sun.com	2. Sun site for patches and security fixes.
	3. http://www.cisecurity.com/bench_solaris.html	3. Center for Internet security (CIS offshoot of SANS) site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
	4. http://csrc.nist.gov/pcig/STIGs/unix-stig-v4r4-091503.zip	4. Defense Information Systems Agency (DISA) Unix configuration guidelines. Contains information for general UNIX security and specifications for Solaris.
	5. http://csrc.nist.gov/pcig/CHECKLISTS/unix-checklist-03152005.zip	5. DISA UNIX Security Checklist.
	6. http://csrc.nist.gov/pcig/CHECKLISTS/01-20-2004-DOT-SBCS-Solaris.doc	6. DISA Solaris Security Checklist.
Windows 2000	1. http://csrc.nist.gov/pcig/CHECKLISTS/win2k-checklist-042205.zip	1. DISA Windows 2000 Security Checklist.
	2. http://csrc.nist.gov/pcig/CHECKLISTS/01-20-2004-DOT-SBCS-Win2K.doc	2. DOT Windows 2000 Secure Baseline Configuration Standards Checklist.
Windows 2000 Windows NT Windows XP	1. http://www.cisecurity.com/bench_win2000.html	1. CIS site for system vulnerability assessment and configuration guidelines. Includes benchmark testing tool and technical information.
	3. http://csrc.nist.gov/pcig/STIGs/windows-2k-xp-2003-addendum-v5r0_3.pdf	2. DISA Windows NT/2000/XP Addendum.
Windows 2003 Windows XP Windows 2000 Windows NT 4.0	http://www.nsa.gov/snac/downloads_all.cfm	NSA guidelines for Windows security developed by NSA's Systems and Network Attack Center (SNAC).

System Type	Standards and Checklists Available	Comments
Windows 2003 Windows XP Windows 2000 Windows NT 4.0 SQL Server IIS	1. http://www.microsoft.com/technet/Security/default.mspx 2. http://www.microsoft.com/technet/security/tools/mbsahome.mspx	Microsoft security site and a link to the Microsoft Baseline Security Analyzer (MBSA). MBSA includes a graphical and command line interface that can perform local or remote scans of Windows operating systems. MBSA runs on: Windows 2000, Windows XP, and Windows Server 2003 systems. MBSA will scan for common system misconfigurations in the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS), SQL Server, Internet Explorer, and Office. MBSA will also scan for missing security updates for the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, IIS, SQL Server, Internet Explorer, Office, Exchange Server, Windows Media Player, Microsoft Data Access Components (MDAC), MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, and Host Integration Server.
Windows NT	1. http://csrc.nist.gov/pcig/STIGs/NSA-Windows-NT-Guide.zip	1. DISA NSA Windows NT Guide STIG.
	2. http://csrc.nist.gov/pcig/STIGs/ntwin2k-addendumv3r1-112602.doc	2. DISA Addendum to the NSA Guide to Securing Windows NT STIG.
	3. http://csrc.nist.gov/pcig/CHECKLISTS/winnt-checklist-042205.zip	3. DISA Windows NT Security Checklist.
Windows XP	1. http://csrc.nist.gov/pcig/STIGs/winxp_STIG_NSA.pdf	1. DISA Windows XP Guide.
	2. http://csrc.nist.gov/pcig/CHECKLISTS/winxp-checklist-042205.zip	2. DISA Windows XP Security Checklist.
	3. http://csrc.nist.gov/itsec/guidance_WinXP.html	3. Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist - Special Publication 800-68 (Draft).
Routers		
CISCO	1. http://www.cisco.com	1. CISCO Web site.
	2. http://www.nsa.gov/snac/downloads_all.cfm	2. NSA guidelines for Cisco security developed by NSA's Systems and Network Attack Center (SNAC).
	3. http://www.cisecurity.com/bench_cisco.html	3. CIS site for system vulnerability assessment and configuration guidelines. Includes technical information on Oracle security configurations.
	4. http://csrc.nist.gov/pcig/CHECKLISTS/cisco-router-checklist.doc	4. CISCO IOS Router Checklist.

System Type	Standards and Checklists Available	Comments
Juniper	http://csrc.nist.gov/pcig/CHECKLISTS/juniperrouterchecklistv5r2_1-062504.doc	DISA STIG for Juniper routers, a supplement to the Network Infrastructure Checklist.
Miscellaneous		
Application Security	1. http://csrc.nist.gov/pcig/CHECKLISTS/appsec_checklist_2.1.6_15apr05.doc	1. DISA Application Security Checklist.
	2. http://csrc.nist.gov/pcig/CHECKLISTS/desktop_app_checklist_v1r19.zip	2. DISA Desktop Application Security Checklist.
	3. http://csrc.nist.gov/pcig/STIGs/Desktop-Application-STIG-V2R1.pdf	3. DISA Desktop Application STIG.
Biometrics	1. http://csrc.nist.gov/pcig/CHECKLISTS/biometric_checklist_082304.doc	1. Biometrics Checklist.
	2. http://csrc.nist.gov/pcig/STIGs/biometrics-stig-v1r2.pdf	2. Biometrics STIG.
	3. http://csrc.nist.gov/pcig/STIGs/scan_Biometrics-Final-STIG-Memo-V1R1-Memo.doc	3. Department of Defense Biometrics STIG.
DNS	1. http://csrc.nist.gov/pcig/CHECKLISTS/dns_v2r1.1_checklist_final_05122004.doc	1. DISA DNS Checklist.
	2. http://csrc.nist.gov/pcig/STIGs/dns_stig_v2r2.pdf	2. DISA DNS STIG.
ESM Security	http://csrc.nist.gov/pcig/STIGs/esm_stig_v1r0.pdf	DISA Enterprise System Management (ESM) STIG.
Peripherals	1. http://csrc.nist.gov/pcig/STIGs/peripheral-stig-v1r0.pdf	1. DISA Peripheral STIG.
	2. http://csrc.nist.gov/pcig/STIGs/span-stig-v1r1.pdf	2. DISA Sharing Peripherals Across the Network STIG.
Remote Computing	http://csrc.nist.gov/pcig/STIGs/secureremotecomputing-stig-v1r1-021403.doc	DISA Secure Remote Computing STIG.
Tandem	1. http://csrc.nist.gov/pcig/CHECKLISTS/tandem-chklstv2r1-1-090203.doc	1. DISA Tandem Checklist.
	2. http://csrc.nist.gov/pcig/STIGs/tandem_stig_v2r2.pdf	2. DISA Tandem STIG.
VM	1. http://csrc.nist.gov/pcig/STIGs/virtual-machine_stig_v2r2.pdf	1. DISA Virtual Machine (VM) STIG.

System Type	Standards and Checklists Available	Comments
	2. http://csrc.nist.gov/pcig/CHECKLISTS/vmchklst-v2r11-jul03.doc	2. DISA VM Checklist.
VoIP	http://csrc.nist.gov/pcig/CHECKLISTS/voip-checklist-073004.doc	DISA VoIP Security Checklist.
Web Security	1. http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_v4.1.6_april05.zip	1. DISA Web Server Security Checklist.
	2. http://csrc.nist.gov/pcig/STIGs/Web-STIG-V5R1.pdf	2. DISA Web Server STIG.
Wireless	1. http://csrc.nist.gov/pcig/STIGs/Wireless-STIG-V3R1.zip	DISA Wireless STIG.
1.1.1.1.1.1	2. http://csrc.nist.gov/pcig/STIGs/mobile-computing-addendum-v1r0.doc	DISA Mobile and Wireless Addendum to the Wireless STIG.
1.1.1.1.1.2	3. http://csrc.nist.gov/pcig/CHECKLISTS/wireless-checklist-v3r11.doc	DISA Wireless Checklist.
1.1.1.1.1.3	4. http://csrc.nist.gov/pcig/CHECKLISTS/wlan-sec-framewrk-jan04.pdf	DISA Wireless LAN Security Framework.
1.1.1.1.1.4	5. http://csrc.nist.gov/pcig/CHECKLISTS/wlan-sec-framewrk-jan04.pdf	DISA Wireless LAN Security Framework Addendum to the Wireless STIG.

3.10.2 - National Institute of Standards and Technology (NIST)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program.

Under the Computer Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards Publications (FIPS), Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-XX) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of the Federal Information Security Management Act (FISMA) of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, references to the "waiver process" contained in many of the FIPS are no longer operative. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST publications for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are incorporated into the CMS CSRs. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program. Table 3.3 contains a listing of NIST publications relevant to common systems or technology utilized within the Medicare business partner community. Table 3.3 is not meant to be all-inclusive and may contain some references that are not applicable to a particular Medicare business partner application. The most current NIST publications can be found at http://csrc.nist.gov/publications/index.html.

Table 3.3. NIST Publications

Publication Number	Title
SP 800-79 (Draft)	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-77 (Draft)	Guide to IPsec VPNs
SP 800-76 (Draft)	Biometric Data Specification for Personal Identity Verification
SP 800-73	Interfaces for Personal Identity Verification
SP 800-72	Guidelines on PDA Forensics
SP 800-70	The NIST Security Configuration Checklists Program
SP 800-68 (Draft)	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-64	Security Considerations in the Information System Development Life Cycle
SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
SP 800-61	Computer Security Incident Handling Guide
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-58	Security Considerations for Voice Over IP (VoIP) Systems
SP 800-57 (Draft)	Recommendation on Key Management
SP 800-56 (Draft)	Recommendation on Key Management
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53	Recommended Security Controls for Federal Information Systems
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Windows 2000 Professional
SP 800-42	Guideline on Network Security Testing
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-40	Procedures for Handling Security Patches
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-38B	Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode

Publication Number	Title
SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
SP 800-36	Guide to Selecting Information Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-31	Intrusion Detection Systems (IDS)
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-27 Rev. A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21	Guideline for Implementing Cryptography in the Federal Government
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-19	Mobile Agent Security
SP 800-18	Guide for Developing Security Plans for Information Technology Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC)
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook
FIPS 201	Personal Identity Verification for Federal Employees and contractors
FIPS 200 (Draft)	Minimum Security Requirements for Federal Information and Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Advanced Encryption Standard
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 191	Guideline for The Analysis of Local Area Network Security
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 188	Standard Security Labels for Information Transfer
FIPS 186-2	Digital Signature Standard (DSS)
FIPS 185	Escrowed Encryption Standard
FIPS 181	Automated Password Generator
FIPS 180-2	Secure Hash Standard (SHS)
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 113	Computer Data Authentication

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

4.0 - IT Systems Sensitivity/Criticality Determinations

(Rev. 3, 03-28-03)

The systems security efforts of the CMS Business Partner Security Program are based on the sensitivity of data contained in IT systems, and the operational criticality of the data processing capabilities of those systems. Security level designations are used to define the requirements of security efforts to protect CMS's information assets. Some of CMS's most critical information assets are the data recorded in these assets, such as financial, Medicare, Federal Tax Information (FTI), beneficiary eligibility, and hospital and medical claims.

4.1 - Information Security Levels

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

- The sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse)

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

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

Table 4.1. Summary of Sensitivity and Criticality Levels

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

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

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

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

- Confidentiality. The system contains information that requires protection from unauthorized disclosure.

- Integrity. The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including the detection of such activities.

- Availability. The system contains information or provides services that must be available on timely basis to meet mission requirements or to avoid substantial losses.

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

4.1.1 - Sensitivity Levels for Data

(Rev. 3, 03-28-03)

Sensitivity levels are assigned to data based on the highest level of sensitivity of the data and the requirements of specific laws governing the protection or disclosure of information (e.g., the Privacy Act and the HIPAA privacy and security regulations).

4.1.1.1 - Level 1: Low Sensitivity

(Rev. 3, 03-28-03)

This category identifies data that requires minimal protection. Threats to this data are minimal, and only minimal precautions to protect the data need to be taken. Unintentional alteration or destruction is the primary concern for this type of data. This category includes any of the following:

Data only in its raw form, such as in some laboratory research applications, and the computerized correspondence and documents in some offices.
Automated Systems of Records, which contain information that is virtually in the public domain, such as employee locator files, and for which any unauthorized disclosures could be expected not to adversely affect the individual.

4.1.1.2 - Level 2: Moderate Sensitivity

(Rev. 3, 03-28-03)

This category identifies data that has importance to CMS and its business partners, and which must be protected against such acts as malicious destruction. However, because this type of data is most often collected for analytical purposes, disclosure problems are not usually significant. This category includes any of the following:
Management information concerning workload, performance, staffing, and similar data, usually in statistical form, which is used to generate reports that reflect the status of an organization. Access to this data needs to be restricted only to a limited degree. The data is protected because of its value to the organization but is intended for disclosure in some form eventually.
Research and statistical data accumulated to provide information about CMS programs to the public. This data needs protection commensurate with the value of the information to the organization. Loss of this kind of data would not normally be potentially embarrassing or detrimental either to an individual or to the organization.
Automated systems of records subject to the Privacy Act, which contain information not in the public domain, but for which unauthorized disclosure could cause nonspecific embarrassment to an individual.
Computerized correspondence and documents, which must be protected from unauthorized alteration or disclosure. These types of data include all correspondence, memoranda, and other documents whose release or distribution outside the Federal government or within the organization needs to be controlled.

4.1.1.3 - Level 3: High Sensitivity

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This category identifies the most sensitive unclassified data processed within CMS and business partner IT systems. This category of data is referred to as sensitive information within the CMS CSRs. Data in this category requires the most stringent and the greatest number of information security safeguards at the user level. This category includes, but is not limited to, the following:

- Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

- Any data that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act (FOIA).

- All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the FOIA; i.e., for which unauthorized disclosure would constitute a “clearly unwarranted invasion of personal privacy” likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing. This data includes, but is not limited to, FTI, including all Federal Tax Return information.

- All electronic health care information and individually identifiable health care information as specified in the regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Payment information that is used to authorize or make cash payments to individuals or organizations. This data is usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter to cause an improper payment.

- Medicare proprietary information that has value in and of itself, and which must be protected from unauthorized disclosure.

- Computerized correspondence and documents that are considered highly sensitive or critical to an organization and which must be protected from unauthorized alteration or premature disclosure.

Proprietary information that has value in and of itself and that must be protected from unauthorized disclosure.

4.1.1.4 - Level 4: High Sensitivity and National Security Interest

(Rev. 3, 03-28-03)

The CMS currently processes no information in this category. This category identifies all databases that contain national security classified information and all databases that contain other sensitive but unclassified information, the loss of which could adversely affect national security interests.

4.1.2 - Criticality Levels for IT Systems

(Rev. 3, 03-28-03)

Criticality levels are assigned to systems based upon the relative importance of their processing capabilities to the organizations they support. A Level 1 designation is used for a system with the lowest criticality of data processing relative to the organization it supports; and a Level 4 designation is used for a system with the highest criticality.

4.1.2.1 - Level 1: Low Criticality

(Rev. 3, 03-28-03)

This category identifies systems with data processing capabilities that require minimal protection. These include systems that, in the event of alteration or failure, would affect the organization minimally or could be replaced with minimal staff time or expense. This category also includes systems that generate, store, process, transfer, or communicate data that is considered to have low or no sensitivity (Level 1).

4.1.2.2 - Level 2: Moderate Criticality

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
This category identifies systems with data processing capabilities that are considered important but not critical to the internal management of CMS. This category includes the following:

- Systems in which failure to function for an extended period of time would not have a critical impact on the organizations they support.

Systems that generate, store, process, transfer, or communicate data that is considered to have moderate sensitivity (Level 2).

4.1.2.3 - Level 3: High Criticality

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
This category identifies systems with data processing capabilities that are considered critical to CMS. This category includes the following:

- Systems whose failure to function for even a short period of time could have a severe impact on CMS or the organizations that they support.

- Systems that perform functions with data that are considered to have a high potential for fraud, waste, or abuse.

Systems that generate, store, process, transfer, or communicate data that is considered to have high sensitivity (Level 3) and categorized as sensitive information.

4.1.2.4 - Level 4: High Criticality and National Security Interest

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
This category identifies all systems with data processing capabilities that are considered critical to the well being of the CMS organization. An example would be systems that handle sensitive-but-unclassified information, the loss of which could adversely affect national security interests. National security directives and other Federal government directives require that these systems be protected in proportion to the threat of compromise or exploitation and the associated potential damage to the interest of CMS, its customers, and personnel.

4.2 - Sensitive Information Protection Requirements

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
Business partners are responsible for implementing a Minimum Protection Standard (MPS) for all CMS Level-3 – High-Sensitivity (CMS sensitive) information and materials. The MPS applies to all IT facilities, areas, or systems processing or storing CMS sensitive information in any form or on any media. The following chart should be used to determine the minimum standards required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The following alternative methods are not listed in any order of preference or security significance.

Table 4.2. Protection Alternative Chart

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

Because local factors may require additional security measures, management must analyze local circumstances to determine space, container, and other security needs at individual facilities. The

MPS has been designed to provide management with a basic framework of minimum security requirements.
The objective of these standards is to prevent unauthorized access to CMS sensitive information.
MPS requires two barriers to accessing sensitive information under normal security:

Alternative #1: secured perimeter and locked container
Alternative #2: locked perimeter and secured interior
Alternative #3: locked perimeter and security container.

Locked means a perimeter, area, or container that has both a lock and keys or combinations that are controlled. A security container is a lockable metal container with a resistance to forced penetration, with both a security lock and keys or combinations that are controlled. (See the following sections for additional explanation and details on these requirements.)
The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information must be containerized in areas where other than authorized employees may have access after hours (e.g., security personnel or custodial service personnel).

4.2.1 - Secured Area

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

A secured or restricted area is one whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas must either meet secured area criteria **or** provisions must be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information.
Restricted areas will be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance must have controlled access (electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

4.2.2 - Security Room

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (normal construction material, permanent in nature, such as masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room must be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking Systems for Secured Areas and Security Rooms).
Additionally, any glass in doors or walls will be security glass [at least two layers of 1/8-inch plate glass with .060-inch (1/32) vinyl interlayer, nominal thickness shall be 5/16-inch]. Plastic glazing material is not acceptable. Vents and louvers will be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that will annunciate at a protection console, UL-approved central station, or local police station; it will be given top priority for guard/police response during any alarm situation.
Cleaning and maintenance should be performed in the presence of an employee authorized to enter the room.

4.2.3 - Secured Interior/Secured Perimeter

(Rev. 4, 03-05-04)
Secured areas are internal areas that have been designed to prevent undetected entry by unauthorized persons during non-working hours. Secured areas/ secured perimeters must meet the following minimum standards:
Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, **or** any lesser-type partition (i.e., slab-to-slab walls) supplemented by UL-approved electronic IDS and fire detection systems.
Unless electronic IDS devices are used, all doors entering the space must be locked, and strict key or combination control should be exercised.
In the case of a fence and gate, the fence must have IDS devices **or** be continually guarded, and the gate must be either guarded or locked with intrusion alarms.
The space must be cleaned during working hours in the presence of a regularly assigned employee.

4.2.4 - Container

(Rev. 4, 03-05-04)
The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, and any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 - Locked Container

(Rev. 4, 03-05-04)
Locked containers must include lock mechanisms that use either a built-in key, or hasp and lock, and include the following features: (1) metal cabinet or box with riveted or welded seams, or (2) metal desks with locking drawers.

4.2.4.2 - Security Container

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. Combinations for combination locks will be given only to those individuals who have a need to access the container. Security containers include the following:

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

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

4.2.4.3 - Safes/Vaults

(Rev. 4, 03-05-04)
A safe/vault is not required for storage of CMS sensitive information. However, if one is used for such storage, it must be located within a secured or locked perimeter type and it must meet the following requirements:

- A safe is a GSA-approved container of Class 1, IV, or V, or UL listings of TRTL-30, TXTL-60, or TRTL-60.

- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, that uses UL-approved vault doors and meets GSA specifications.

4.2.5 - Locking Systems for Secured Areas and Security Rooms

(Rev. 4, 03-05-04)
Minimum requirements for locking systems for Secured Areas and Security Rooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock.

- Have a deadbolt throw of one inch or longer.

- Double-cylinder design. Cylinders are to have five or more pin tumblers.

- If bolt is visible when locked, it must contain hardened inserts or be made of steel.

- Both key and lock must be "off-master."

- Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours.

- Keys to secured areas not in the personal custody of an authorized employee and all combinations will be stored in a security container.

4.2.6 - Intrusion Detection System (IDS)

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)
Physical Intrusion Detection Systems are designed to detect attempted perimeter area breaches. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection during non-working hours. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, and are designed to set off an alarm at a given location when the sensor is disturbed.

5.0 - Internet Security

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)
Transmission of and/or receipt of health care transactions (claims, remittances, etc.) or other CMS sensitive data over the Internet is prohibited at Medicare business partners (or their agents). Practically, this prohibition means that CMS requires the use of private networks or dial-up connections with any entity that transmits or receives health care transactions and/or CMS

sensitive data to or from the Medicare contractor. CMS is closely following the health care industry's movement toward adoption of industry-wide security technologies that ensure confidentiality, integrity, and availability of data moved over the Internet and will reconsider its policy at the appropriate time.

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

Table of Contents
(Rev. 7, 03-17-06)

1.0 - Introduction to the CMS Integrated Security Suite (CISS)

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

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

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

2.0 - CISS Self-Assessment (CAST) Module

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

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

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

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

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

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

2.1 - Applicable Laws

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

CMS CSRs http://www.cms.hhs.gov/manuals/downloads/117_systems_security_AtchA.pdf detail technical requirements for CMS Business Partners who use information systems to process Medicare data. Business partners must establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data.

The CMS CSRs are developed by assessing and analyzing requirement statements from a number of Federal and CMS mandates, including the following:

- *Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.*

  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- *OMB Circular No. A-127, Financial Management Systems, June 21, 1995.*

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

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

  http://www.whitehouse.gov/omb/circulars/a127transmittal2.html

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

  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

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

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

- *Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources, December 17, 2003.*

  http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf

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

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

- *NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.*

  http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

- *CMS System Security Plans (SSP) Methodology, Draft Version 3.0, November 6, 2002.*

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

- *CMS Information Security Risk Assessment Methodology, Version 2.1, April 22, 2005.*

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

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

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

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

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

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

  http://aspe.os.dhhs.gov/admnsimp/pl104191.htm
  http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm

2.2 - CSR Categories

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

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

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

Table A-1. CSR Category Descriptions

2.3 - CSR Elements

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

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

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

Table A-2. CSR Elements

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

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

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

- ***Protocols**. Recommended procedures designed to verify that a site is in compliance with system security requirements. Protocols are not security requirements; rather, they have been developed based on the same Federal and CMS security documents used to create the CSRs. As such, they provide Business Partners with Self-Assessment procedures that are similar to audit procedures used by CMS and external agencies. This information is available in the CISS during the Self-Assessment process and may be printed from the Reports menu.*

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

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

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

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

Applicability legend:

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

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

- *Where Federal improvements are already covered by an existing CSR, these documents are added as references.*

- *Where Federal improvements are partially covered by an existing CSR, the existing CSR is modified to incorporate appropriate language and the appropriate document(s) are listed as reference(s).*

- *Where Federal improvements are not covered by an existing CSR, a new CSR is added and the appropriate document(s) are listed as a reference(s).*

At the present time, CMS does not anticipate any additional funding being provided to Business Partners to address any new requirements. Any new requirements represent best practices, and CMS believes many Business Partners are already compliant or in the process of implementing changes to become compliant.
Where the implementation of alternatives and/or compensating controls is not possible, a Business Partner's non-compliance must also be documented in the Risk Assessment (RA), System Security Plan (SSP), and the CISS Self-Assessment. CMS encourages Business Partners to fund these requirements by reallocating/reprogramming current fiscal year resources. CMS also recognizes that there are times when controls cannot be implemented due to resource issues. Alternative or compensating safeguards can be implemented to reduce the risks to CMS and its systems. This must be considered part of risk management and the alternative or compensating controls must be documented in the information security risk assessment, SSP, and annual CISS Self-Assessment submissions.

2.4 - Completing the Self-Assessment (CAST)

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

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

2.5 - All Responses

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

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

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

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

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

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

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

f) *Each CSR in the CISS includes an Applicability matrix, which identifies the likely responsibility for each CSR by CMS contract type (i.e., Part A, Part B, DMERC, etc.). The purpose of the Applicability matrix is not to summarily include or exclude CSRs from a particular contract type. The Applicability matrix is designed to be used as a guide to Business Partners. CMS recognizes that system configurations vary widely throughout the Business Partner community; therefore, each Business Partner must evaluate and report on each CSR's applicability to its own systems.*

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

application) that manipulates data or performs a specific function (e.g., front-end and back-end applications).

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

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

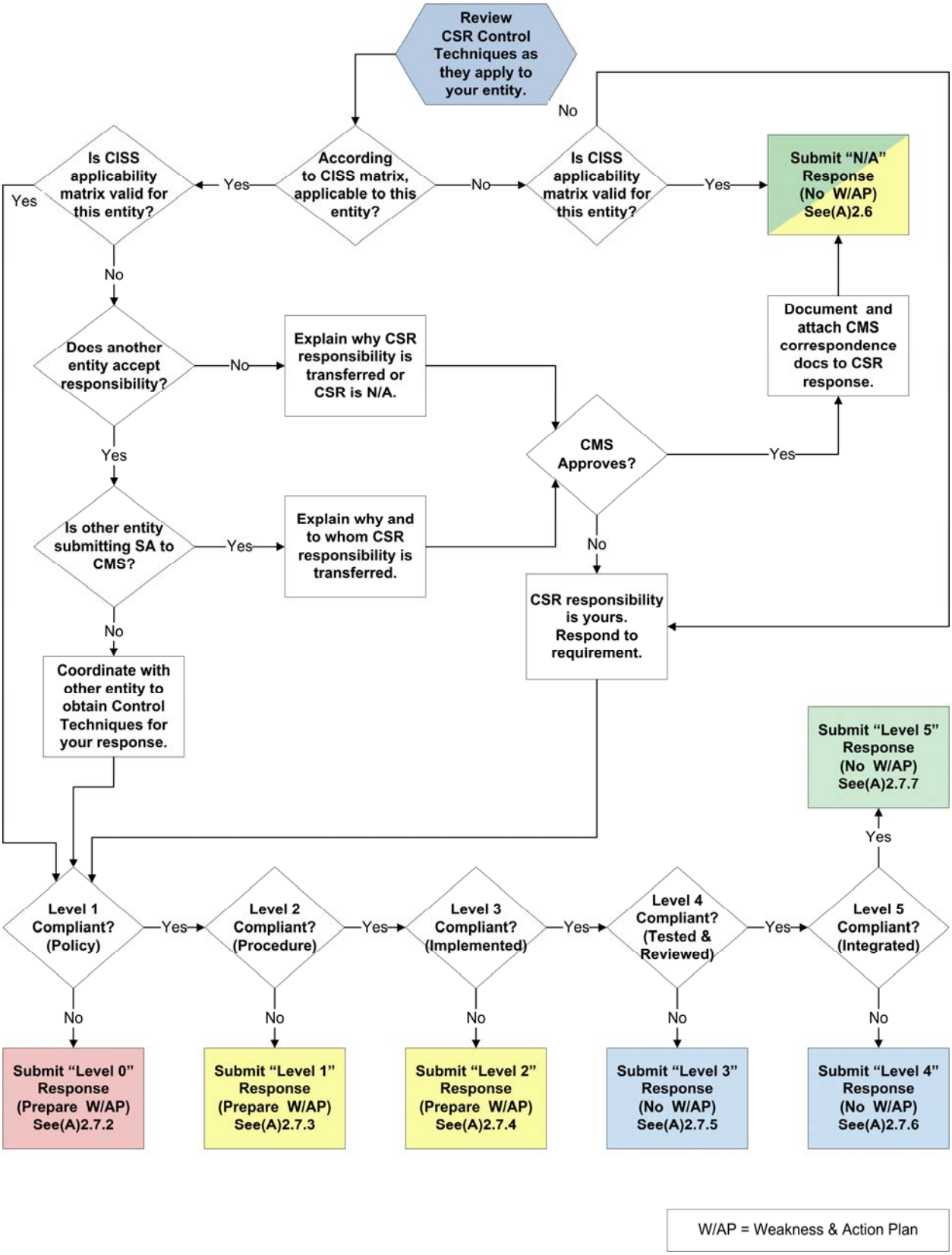

Figure A-1. Response Status Decision Tree

2.6 - "N/A" Response Status

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

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

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

b) ***How** did you verify this status with CMS?*
i. Applicability matrix says CSR is NOT applicable. CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability matrix.
ii. Applicability matrix says CSR is applicable. In the case of an "N/A" response that is not corroborated by the Applicability matrix, CMS approval must be obtained and documented, and such documentation must be provided with the CSR response (see below). Note that CMS approval must be renewed each year for each "N/A" CSR to be waived.
The CISS tool will require that copies of the associated CMS approval documentation be attached to the CSR response within the CISS tool. Approvals for prior years may be cited in your request for CMS approval for the current year response, but cannot be used as documentation of CMS approval for the current year CSR "N/A" response. Each year, the CMS approval process must be repeated (unless specifically stated in the CMS-provided approval documentation).
Include the following information with CMS-approved "N/A" responses, in addition to the requirements stated above in 2.6(a):
(1) Date CMS approved the response,
(2) CMS office that approved the response, and
(3) Attached documentation of CMS concurrence (e-mail text file, or letter/document).

Example entry for a CMS-approved CSR with a response status of "N/A":
"This requirement describes the required features of 'security rooms.' CSR 2.2.25 suggests 'security rooms' as one of several possible methods, but does not require one. We use 'secured areas' and 'appropriate containers' (CSRs 2.2.19 and 2.2.5). This issue was discussed via letter to CMS (05/15/05) and agreed to by the CMS SSG (06/80/05). Both letters are attached to this

CSR response and are on file in cabinet #3 in the Security Office located on the third floor of Bldg. #3."

2.7 - Five Levels of Security Effectiveness

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

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

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

Table A-3. Levels of Security Effectiveness

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

- ***a.) Weaknesses.*** *Currently, each CSR must minimally be at Level 3 (or above) to be considered in compliance. For any response at Level 2 or below, the [Weakness] button on the CISS Self-Assessment form is enabled. An appropriate Weakness/Action Plan combination must accompany any CSR response at Level 2 or below. However, CMS does not consider a CSR response to be at full maturity until Level 5 is achieved. The CMS goal is to "Strive-for-Five."*
- ***b.) Risk-Based Decision****. In some extreme cases, full implementation of the minimum compliance requirements may present unacceptable fiscal or configuration barriers. In these cases, CMS may agree that the risk is acceptable for the present self-assessment and that no Weakness/Action Plan combination is required nor desired. In such cases, prior CMS concurrence is required AND a full assessment of all of the implications of not meeting each of the minimum 3 levels for the applicable CSR is fully documented in the associated risk-assessment for the system. BOTH the updated risk-assessment AND full documentation of CMS concurrence MUST be attached to the CSR response.*

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

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

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

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

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

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

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

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

i. Do not include planned controls or controls that are not fully implemented. If all components are not fully in place, the response status must be changed to the next lower level and, if required, a suitable Weakness/Action Plan combination identified.
ii. In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.

Example entry for a CSR with a response status of Level 3:
"Security Awareness Training policies and procedures are in-place and such training is conducted during initial employee orientation and every year during the month of November for all employees and contractors. It includes all aspects outlined in the CSR as documented in company policy NG 7541-S3 and associated HR procedures T255, T256, and T257. The records of attendance are maintained in cabinet #5 in the Corporate Training Office, on the fifth floor of Bldg. #5."

2.7.2 - "Level 0" Response Status

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

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

2.7.3 - "Level 1" Response Status

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

Level 1 – Policy – includes:

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

A system is at Level 1 if there is a formal, up-to-date, and documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and

uses monitoring for program effectiveness. Such a policy may be at an organizational level or Medicare claims processing specific.
A documented security policy is necessary to ensure adequate and cost-effective organizational and system security controls. A sound policy delineates the security management structure and clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance.

2.7.4 - "Level 2" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 2 – Procedures – includes:

- *Formal, complete, well-documented procedures for implementing policies established at Level 1.*

- *The basic requirements and guidance issued from applicable public laws; other Federal, department, and agency policy; as well as applicable NIST publications.*

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

2.7.5 - "Level 3" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 3 – Implemented – includes:

- *Security procedures and controls that are implemented.*

- *Procedures that are communicated and individuals are required to follow them.*

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

2.7.6 - "Level 4" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 4 – Tested – includes:

- *Routinely evaluating the adequacy and effectiveness of security policies, procedures, and controls.*

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

Routine assessments and response to identified vulnerabilities are important elements of risk management, which includes identifying, acknowledging, and responding, as appropriate, to changes in risk factors (e.g., computing environment, impact levels) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis. Routine assessments are an important means of identifying inappropriate or ineffective security procedures and controls, reminding employees of their security-related responsibilities, and demonstrating management's commitment to security. Assessments can be performed by Business Partner staff, contractors, or others engaged by CMS management. Independent audits, such as those arranged by the General Accountability Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for assessments initiated by Business Partner management.
To be effective, routine assessments must include tests and examinations of security controls. Reviews of documentation, walk-through of Business Partner facilities, and interviews with Business Partner personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. To be meaningful, assessments should include security controls of interconnected assets (e.g., network supporting applications being tested).
When systems are first implemented or are modified, they should be tested and certified to ensure that the security controls are initially operating as intended. (This would occur at Level 3.) Requirements for subsequent testing and recertification should be integrated into an agency's ongoing test and assessment program.
In addition to test results, Business Partner assessments should consider information gleaned from records of potential and actual security incidents and from security alerts, such as those issued by software vendors. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risks.

2.7.7 - "Level 5" Response Status

(Rev. 7, Issued: 03-17-06, Effective: 05-01-06, Implementation: 05-01-06)
Level 5 – Integrated – includes:

- *A comprehensive security program that is an integral part of a Business Partner's organizational culture.*

- *Decision-making based on cost, risk, and mission impact.*

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

- *Improving security program,*

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

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

2.8 - Findings and Weaknesses

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

Weaknesses form the basis for CISS Action Plans (see section 2.9 of this appendix for a description of Action Plans). Findings and non-compliant CSRs form the basis of Weaknesses. Every Finding and every non-compliant CSR must be addressed by a Weakness record in the CISS. A Finding is any deficiency identified and reported during an audit or review—whether internal or external. For example:

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

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

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

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

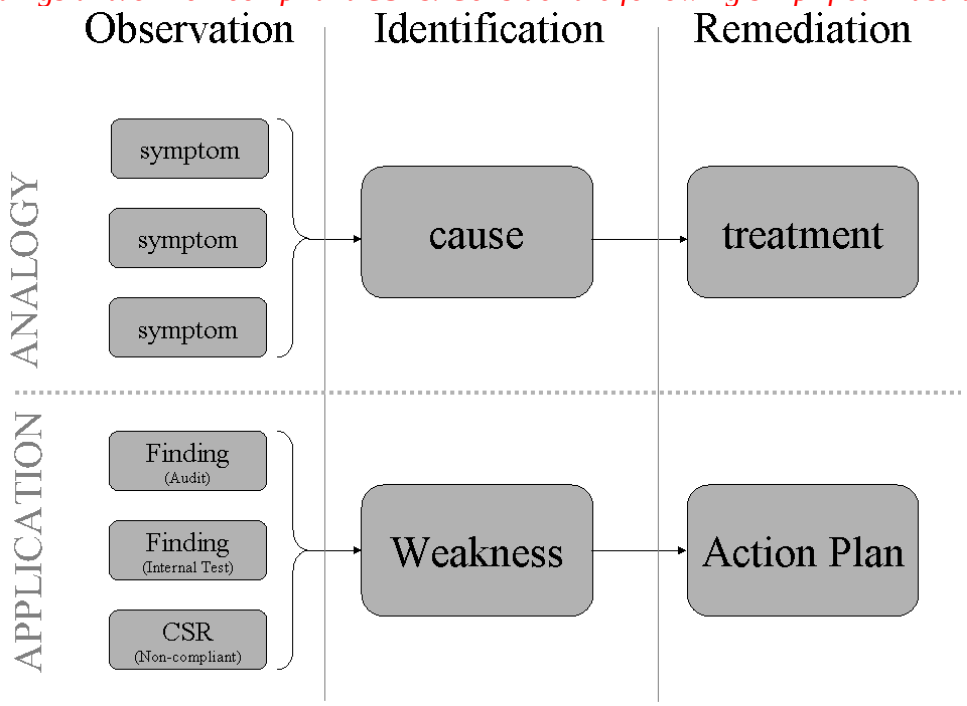

Figure A-2. Analogy for Finding-Weakness-Action Plan Relationship

An Action Plan must be designated to address each Weakness.

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

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

This list is not exhaustive; there are many avenues for discovering Weaknesses. Because the CISS is used to conduct Self-Assessments as well as a repository for IT audit findings, a distinction is made between Weaknesses that are initiated due to non-compliant CSRs during a Self-Assessment and those initiated from any other type of audit or review. In the CISS, any Weakness that does not result from a self-assessment non-compliant CSR is considered to have resulted from some type of audit or review This distinction becomes important when following the flow in Figure A-3, which shows how security-related Weaknesses are linked and reported. The CMS business rules (and the CISS tool) require that all Weaknesses be associated with at least one non-compliant CSR response. It is expected that a Weakness will often be associated with both audit Finding(s) and at least one non-compliant CSR(s). In such cases, the flow in Figure A-3 must be followed through both paths after the first decision to ensure that the Weakness is linked to all applicable CSRs and Findings.

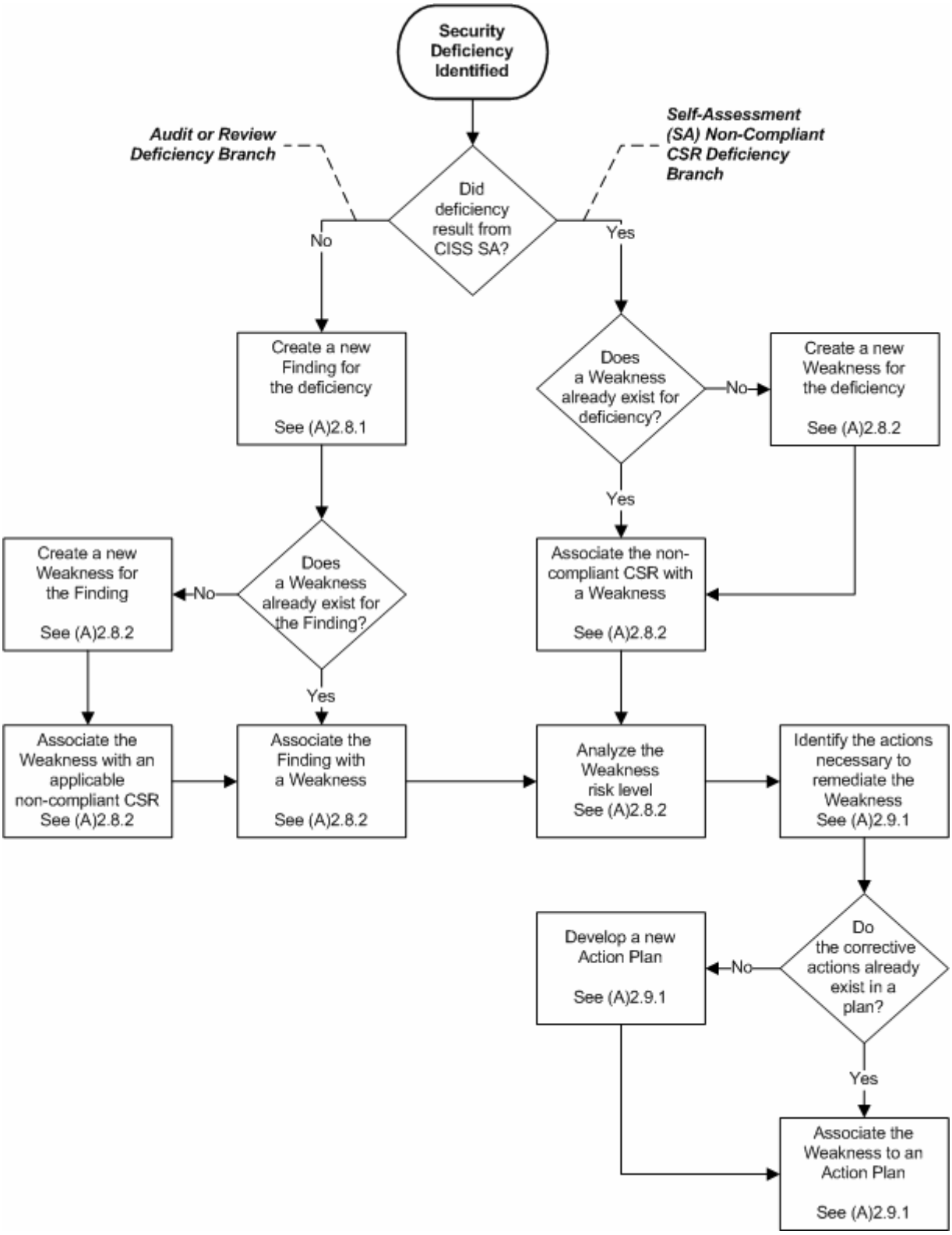

Figure A-3. Weakness Decision Tree

2.8.1 - Findings

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

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

2.8.1.1 - Finding Identifier

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

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

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

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

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

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

- *R - Accounts Receivable review*
- *C - CPIC, (your annual self certification package)*
- *E - CFO EDP review*
- *F - CFO Financial review*
- *S - Statement on Auditing Standards no. 70 (SAS 70)*
- *O - OIG reviews (HHS Office of Inspector General [Information Technology] controls assessment)*
- *G - GAO reviews (financial reviews)*
- *P - CMS 1522 workgroups reviews*

- *V - CFO related NVA/ST*
- *N - SAS 70 Novation;*
- *M - CMS CPIC workgroup reviews*
- *9T - Section 912 Testing*
- *9E - Section 912 Evaluations*
- *AC - CMS self-assessment Annual Compliance Audits*
- *IR - Internal reviews initiated by the entity to meet other Federal requirements, and*
- *RA - Issues identified during routine risk assessments.*

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

2.8.1.2 - Finding Title and Description

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

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

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

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

2.8.1.3 - Finding Status

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

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

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

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

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

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

2.8.1.4 - Determination of Finding Risk Level

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

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

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

2.8.1.5 - Finding FMFIA and CPIC Severity

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

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

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

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

2.8.1.6 - Finding Category

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

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

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

2.8.1.7 - Finding Point(s) of Contact

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

For each Finding reported, a primary POC must be selected. While multiple POCs can be assigned to a Finding, only one POC can be designated as primary for each Finding. The

primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Finding. Non-primary POCs can include anyone who will assist the primary POC in resolving the Finding.

2.8.2 - Weaknesses

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

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

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

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

2.8.2.1 - Weakness Identifier

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

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

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

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

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

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

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

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

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

2.8.2.2 - Weakness Title and Description

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

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

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

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

2.8.2.3 - Weakness Category

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

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

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

- *Audit Trails.*

2.8.2.4 - Determination of Weakness Risk Level

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

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

2.8.2.5 - Weakness FISMA Severity

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

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

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

The three FISMA Severity levels are:

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

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

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

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

2.8.2.6 - Weakness Type

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

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

- ***Program Weakness**. A Program Weakness impacts multiple IT systems as a result of a deficiency in the IT security program.*

- ***System Weakness***. *A System Weakness pertains to the management, operation, or technical controls of a specific IT system.*

2.8.2.7 - Weakness Status

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

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

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

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

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

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

2.8.2.8 - Weakness Point(s) of Contact

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

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

2.8.2.9 - Determining Risk

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

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

While both system and business risk measurements are discussed and combined in the CMS RA Methodology document, risk determinations made in and by the CISS are for systems only. The

system risk level is derived by combining the threat likelihood value and threat impact value for a specific threat/vulnerability pair, as follows:

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

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

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

2.8.2.9.1 - Likelihood

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

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

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

Table A-4. Likelihood Levels

2.8.2.9.2 - Impact

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

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

Magnitude of Impact	***Impact Definition***
High	*The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.* *Amplification: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the*

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

Table A-5. Magnitude of Impact Definitions

2.8.2.9.3 - Overall Risk

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

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

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

Table A-6. Overall Risk Matrix

2.9 - Action Plans and POA&Ms

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

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

The CISS assists Business Partners in reporting Weaknesses, preparing Action Plans, and submitting the required POA&Ms to CMS. The POA&M submission process is automatic, in that it contains information already entered into the CISS. Therefore, no further guidance is required

beyond the instructions found in section 11, Submissions to CMS, of the CISS User Guide. The remainder of this section is devoted to guidance for populating the CISS Action Plan form.

2.9.1 - Completing Action Plans

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

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

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

2.9.1.1 - Action Plan Title and Description

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

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

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

2.9.1.2 - Determining Completion Dates

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

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

2.9.1.3 - Determining Costs

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

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

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

- *Risk assessment*
- *Security planning and policy*
- *Certification and accreditation*
- *Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)*
- *Authentication or cryptographic applications*
- *Education, awareness, and training*
- *System reviews/evaluations (including security control testing and evaluation)*
- *Oversight or compliance inspections*
- *Development and maintenance of Business Partner reports to CMS and corrective Action Plans as they pertain to the specific investment*
- *Contingency planning and testing*
- *Physical and environmental controls for hardware and software*
- *Auditing and monitoring*
- *Computer security investigations and forensics*
- *Reviews, inspections, audits, and other evaluations performed on Business Partner facilities and operations.*

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

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

In identifying security costs, Business Partners may find it helpful to ask the following simple question: "If there were no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" If

Business Partners encounter difficulties with the above criteria, they must contact CMS prior to submission of their POA&M report.

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

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

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

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

2.9.1.4 - Determining Funding Sources

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

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

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

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

2.9.1.5 - Milestone Title and Description

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

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

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

2.9.1.6 - Milestones with Completion Dates

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

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

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

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

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

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

2.9.1.7 - Milestone Changes

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

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

Appendix B

Medicare Information Technology (IT)
Systems Contingency Planning

Table of Contents
(Rev. 6, 12-09-05)

1.0 - Introduction

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

CMS business partners are required by CMS CSR 5.2 to develop and maintain a contingency plan. This plan is to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption.

Section 3.4 of this document requires that all CMS Medicare business partners prepare, review, and test their Medicare IT systems contingency plans. All General Support Systems (GSS) and Major Applications (MA) that support critical Medicare operations must be covered by a Medicare IT Systems Contingency Plan (CP).

This document presents the direction for accomplishing Medicare IT systems contingency planning. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an IT systems contingency plan, or updating an existing plan.

The business partner information security risk assessment may be used as a checkpoint to determine if appropriate contingencies have been addressed in the contingency plan.

To ensure the contingency plan is workable, it must be thoroughly and periodically tested.

The simplified diagram in Figure B-1 illustrates the IT systems contingency planning process.

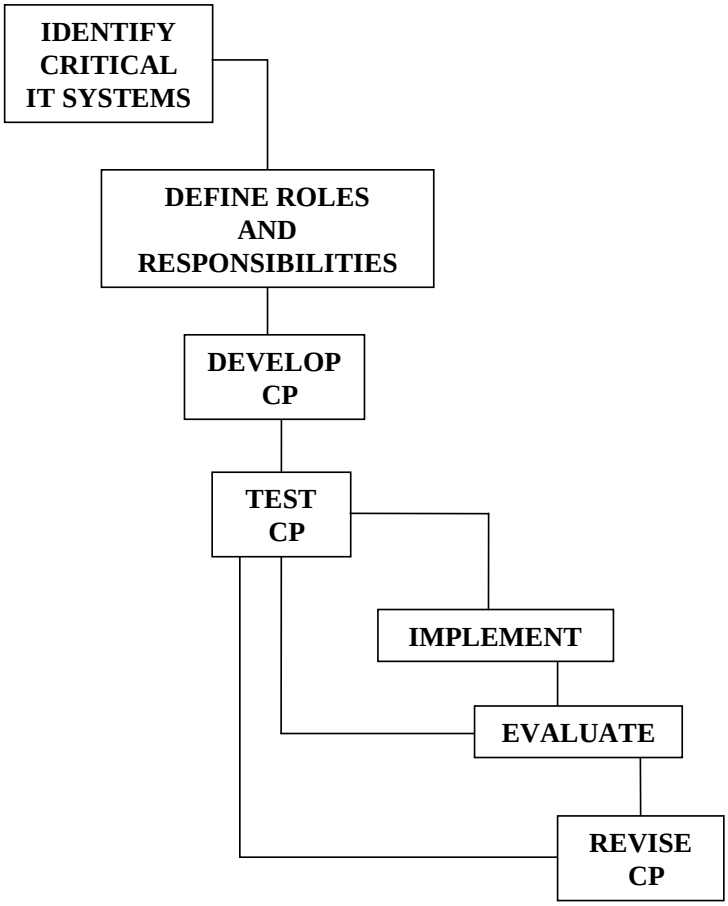

Figure B-1 – IT Systems Contingency Planning Process

2.0 - Scope

(Rev. 3, 03-28-03)
The business partner IT systems contingency plans address organizations and sites where Medicare data is processed, including claims processing locations, data centers, and other processing or printing sites.

3.0 - Definition of an Acceptable Contingency Plan

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
A contingency plan is a document that describes how to plan for and deal with an emergency or system disruption. These situations could be caused by a power outage, hardware failure, fire, or terrorist activity. A contingency plan is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.
Protecting lives is the paramount task while executing a contingency plan.
Before developing an IT systems contingency plan, it is advisable to have or create a contingency policy. The contingency plan must be driven by a contingency policy. The contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.
The IT systems contingency plan should be developed under the guidance of IT management and systems security persons and all organizational components must be actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.
It can be a very subjective argument relative to what constitutes an acceptable contingency plan. In this document, the description of an acceptable contingency plan is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner contingency plans and test reports.
The following summary statements define what constitutes an acceptable contingency plan. This is not an all-inclusive list and the topics are not in any order of importance or priority.

1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.
2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.
3. Considers risk assessment results.
4. Addresses possible and probable emergencies or system disruptions.
5. Can be sufficiently tested on an established regular basis at reasonable cost.
6. Contains information that is needed and useful during an emergency or system disruption.
7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.
8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.
9. Clearly defines the resources necessary to implement the plan.
10. Reflects what can be done – is not a wish list.
11. Assumes people will use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe pressure.

12. Addresses backup and alternate sites.
13. Addresses the use of manual operations, where appropriate and necessary.
14. Contains definitive “Call Lists” to use for contacting the appropriate persons in the proper sequence. This list would include vendor points of contact.

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

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

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

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

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

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

4.0 - Medicare IT Systems Contingency Planning

(Rev. 3, 03-28-03)

The goal of IT systems contingency planning is to continue accomplishing critical Medicare IT systems operations in an emergency or system disruption and to accomplish a rapid and smooth recovery process.

4.1 - Contingency Planning

(Rev. 3, 03-28-03)

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process must address all the actions and resources needed to ensure continuity of operation of critical Medicare IT systems and the means of implementing the needed resources. IT management and staff must be trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located. Contingency planning includes such training.

It is advisable to establish a Medicare IT systems contingency planning team. This team would be responsible for defining critical Medicare IT systems, including applications software, data,

processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 - Coordination With Other Business Partners

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning must include those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links must be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5.0 - Medicare IT Systems Contingency Plan

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The following format may be used in developing an IT system contingency plan. While this format is not required, all of its elements must be included in the Contingency Plan.

1. Introduction
    - Background
    - Purpose/Objective
    - Management commitment statement
    - Scope
        - Organizations
        - Systems
        - Boundaries
    - IT capabilities and resources
    - CP policy
        - Priorities
        - Continuous operation
        - Recovery after short interruption
        - Minimum recovery times
2. Assumptions
3. Authority/References
4. Definition of what the CP addresses
    - Organizations

- Systems
- Boundaries

5. Three phases defined
    - Respond
    - Recover
    - Restore/reconstitute
6. Roles/Responsibilities defined
7. Definition of critical functions
8. Alternate capabilities and backup
9. Definition of required resources to respond and recover
10. Training
    - CP must address Who – When – How
11. Testing the CP
    - Philosophy
    - Plans
    - Boundaries
    - Live vs. Walkthrough
    - Reports
    - Responsibilities
12. CP maintenance/updating

Schedule

13. Relationships/Interfaces
    - Outside (vendors, providers, banks, utilities, services, CMS)
    - Internal
    - Dependencies
14. Attachments
    - Actions for each phase
    - Procedures
    - Call trees
    - Vendor contact list

- Hardware inventory
- Software inventory
- System descriptions
- Alternate/Backup site information
- Assets/Resources
- Risk Assessment Summary (refer to System Security Plans)
- Agreements/Memos of Understanding
- Manual Operations
- Supplies/Materials/Equipment
- Floor plans
- Maps

The contingency plan must provide for off-site storage of:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the contingency plan
- Administrative supplies (forms, blank check stock, etc.).

6.0 - Testing

(Rev. 3, 03-28-03)

The CMS requires testing of the contingency plan annually under conditions that simulate an emergency or a disaster. (CSR Category 5.)

The CMS requires that the critical IT systems must be tested annually and the contingency plan updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 - Claims Processing Data Centers

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

Many of the contractors with which CMS has direct contracts do not have their own data centers. They usually contract this service out. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they must have a contingency plan.

6.2 - Multiple Contractors

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
Data centers usually serve multiple contractors. Existing shared processing environments allow for multiple contractors to process claims at a data center. There are numerous data centers processing Part A and Part B claims for multiple Medicare contractors.
It is important to test a contingency plan at a data center that serves multiple contractors. This provides a mechanism to examine the possible commingling of data between contractors, wherein data may be compromised.
Before testing of the contingency plan begins, it is important to understand how contractor data is protected and/or kept separate. The data centers may use a security package, such as ACF, to control access and separation of data. In order to perform appropriate testing, the complexity of the data center operation must be understood.

6.3 - Test Types

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)
Contingency plan test guidance suggests three types of testing:

Walkthrough
Simulation/modeling
Live.

These are defined below:
Walkthrough: A walkthrough test is accomplished by going thorough a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented in a way that they can be logically followed. A "test team" might sit around a table and talk thorough each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but would not actually start all hardware, software and communication operations in order to assume the function of the primary site.
Simulation/Modeling: Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster, or the number of people that can get to an alternate site following a disaster.
Simulation involves taking some physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team to do the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.
Live: This is the most complete and expensive test to accomplish. It involves doing physically what would actually be accomplished if an emergency occurred. People and materials would be moved to an alternate site for the test. Servers would actually be shut down to reduce capability. Power would actually be shut off. Live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications and people at

the alternate site would be set into action and begin functioning as the primary site to support operations.

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

End-to-end testing can be done as part of walkthrough or live test.

Not testing end-to-end means that some links, processes, or subsystems are missed.

What is the risk in not doing end-to-end testing?

Live end-to-end testing can be very expensive!

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

6.3.1 - Live vs. Walkthrough

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

- High-level testing can take the form of a walkthrough test.
- A walkthrough can be part of the overall testing process, but not the whole process.
- Lower-level testing can include a walkthrough, if live testing is not an option.
  - Live testing should be the first choice.
  - Fall back to a simulation/model if live testing is not an option.
  - Cost, time, and interruption of normal operations are major considerations in doing a live test.
  - A walkthrough test should be the last resort.
    - Ask what a walkthrough test would miss.
    - Consider the ramifications of missing that part of the test.
    - Remember that there is risk in not doing a live test—can the risk be accepted?
  - Consider the criticality of functions, processes, and systems.
  - If critical to continuing essential business operations, then these are strong candidates for live testing.
- Testing interfaces.

  It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a “walkthrough” method. Simulation or “live” testing is preferred.
- Cost and complexity.

  The decision as to how to test critical functions, processes, and systems must result from careful consideration of complexity and cost. A complete “live” test of all elements of an operation may prove to be extremely costly, in terms of both dollars

and time. If that cost out weighs the "cost" of the risk of not doing live testing, then "live" testing should probably be ruled out.

6.3.2 - End-to-End

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

- End-to-end testing must only be considered for critical functions, processes, or systems.
- Why is end-to-end testing needed?
- It provides the best assurance that there are no problems.
- Would a partial test be meaningful?
- If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.
- Examples of types of end-to-end tests:
  - Claims receipt through to check generation
  - Query of a database through to the response
  - MSP check request through to check issue and back to MSP.
- Evaluate complexity and cost.

  The decision on how to test critical functions, processes, and systems must carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost out weighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.
- Consider the criticality of functions, processes, and systems.

  Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.
- If you can't do end-to-end testing, then consider live testing of all links possible to help ensure minimum problems.
  - Or, do simulation/modeling.
  - Or, do walkthrough.

Overall testing may take the form of reviews, analyses or simulations of contingencies. Reviews and analyses may be used for non-critical systems, whereas critical systems should be tested under conditions that simulate an emergency or a disaster.
It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems must be tested.
Testing may include activities in addition to computer processing. Manual operations should be checked according to procedures, and changes made as experience indicates.

6.4 - Local Processing Environments (PCs/LANs)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

IT systems contingency plan testing relative to local environments, such as individual or clustered workstations and LAN configurations, may be less comprehensive than data center testing. Reviews and analyses may be used to accomplish certain non-critical systems testing, whereas critical systems require full simulation or live testing. The criticality of the system is the deciding factor relative to what type testing is used, how often tests are accomplished, and how thorough the testing should be.
The decision of which test approach to use relative to a specific system or configuration must be a management decision based on advice from the SSO, IT systems staff, operations and support representatives, and the lead test planner/manager.

6.5 - Test Planning

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

An IT systems contingency test plan must address at least the following:

- Test objectives
- Required equipment and resources
- Necessary personnel
- Schedules and locations
- Test procedures
- Test results
- Failed tests
- Corrective action management process
- Retest
- Approvals.

It is advisable to establish test teams responsible for preparing and executing the IT systems contingency plan tests. Responsibilities must be assigned to test team members, including executives, observers, and contractors.
Following testing, the corrections specified in a Corrective Action Management Process must be tested. The process must include:

- List of items that failed the previous test
- Corrections planned
- Retest detail
- Schedule
- Review responsibilities.

Ensure that the lessons learned from IT systems contingency plan testing are discussed among senior business partner management, operations, IT management and staff, and the SSO.
Documentation must exist for:

Test plans
Test results
Corrective action management process
Retest plans
Memos of Understanding/Formal Test Arrangements.

7.0 - Minimum Recovery Times

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

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

8.0 - Responsibilities

(Rev. 3, 03-28-03)

Following is a summary of responsibilities for key groups and persons involved with contingency planning.

8.1 - Business Partner Management

(Rev. 5, Issued: 12-23-04, Effective: 10-01-04, Implementation: 02-28-05)

Defines scope and purpose of IT systems contingency planning.
Authorizes preliminary IT systems contingency planning.
Ensures that appropriate contingency plans are developed, periodically tested, and maintained.
Ensures that all IT operations participate in the contingency planning and the development of the plans.
Reviews the plan and recommendations.
Requests and/or provides funds for plan development and approved recommendations.
Assigns teams to accomplish development of test procedures, and for testing the plan.
Reviews test results.
Ensures that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.
Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.

Business partner management must approve:

1. The contingency plan
2. Changes to the contingency plan
3. Test Plans
4. Test results
5. Corrective action management processes
6. Retest Plans
7. Memos of Understanding/Formal Arrangement Documents
8. Changes to storage and backup/alternate site facilities.

8.2 - Systems Security Officer (SSO)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Documents the scope and purpose of IT systems contingency planning
Reconciles discrepancies and conflicts
Evaluates security of backup and alternate sites
Leads the preparation of the contingency plan
Submits the plan and recommendations to management
Monitors implementation of the plan and reports status to management
Ensures all testing of the plan is accomplished as required
Reviews test results
Ensures that the plan is updated based on test results.

8.3 - Service Components (provide support functions such as maintenance, physical security)

(Rev. 3, 03-28-03)

- Maintain physical security forces to respond to emergencies.
- Schedule fire and other emergency drills and monitor effectiveness.
- Develop emergency re-supply procedures for forms, supplies, equipment, and furniture.
- Provide for priority replacement of computer hardware.
- Provide for restoring telecommunications.
- Provide for backup sites and procedures.
- Provide information relative to the availability of recovery sites.
- Develop procedures for documenting inventories of equipment and furniture.
- Provide a list of employees' home addresses and phone numbers.
- Support testing of the plan.

8.4 - Operating Components (IT operations personnel)

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Designate employees for emergency response teams.
Designate employees for backup teams.

Designate employees for recovery teams.
Provide a list of employees' home addresses and phone numbers.
Identify time-critical operations and systems.
Identify critical resources, such as hardware, software, data, communications, facilities, and people.
Identify supplies (forms, blank check stock, etc.) to be stored at alternate sites.
Identify critical data to be backed up offsite.
Provide information on testing requirements.
Accomplish and/or support end-to-end system testing.
Review test results.
Identify critical non-automated data processing operations.
Review basic service organization plans and advise SSO where needs are not met.
Monitor contingency plan implementation and report status to management.

9.0 - Changes

(Rev. 3, 03-28-03)

The contingency plan must be updated whenever one or more of the following events occurs:

New systems or operations added.
Upgrade or replacement of Standard System software.
Hardware or software replacement.
Changed back up/alternate site.
Changed storage facilities.
Removal of existing systems or operations.

10.0 - Attachments

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Materials that are too extensive to be included in the body of the Medicare IT systems contingency plan must be included as attachments. These should be referenced in the contingency plan. These should also be a part of the Site Security Profile (Refer to CSR Category 1). Existing material that facilitates response, backup, and recovery operations should be included as attachments or a pointer provided. Much of this material is bulky and relates to the entire organization. The SSO must ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the contingency plan. Such material includes:

Master inventories of forms, supplies, and equipment
Description of computer hardware and peripherals
Description of applications software
Appropriate security weakness information
Systems and program documentation
Prioritized schedules for computer operations
Communications requirements, especially computer networks.

11.0 - Checklist

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

1. Introduction

   Does the contingency plan contain:

   Background

   Is a history of the plan provided? Are the physical environment and the systems discussed?

   Purpose/Objective

   What does the plan address? Why was it written? What does it aim to accomplish?

   Management Commitment Statement

   Has the contingency plan been approved by management and the SSO? Once the contingency plan is created, reviewed, and ready for distribution, it should be approved by site, operations and information systems management, and the SSO.

   Scope

   Are the boundaries of the plan indicated? What organizations are involved, not involved?

   Organizations

   Systems

   Boundaries

   IT Capabilities and Resources

   Is the focus of the plan on IT systems, capabilities, and resources?

   - Contingency Plan Policy
     - Priorities
     - Continuous operation

   Are there functions, processes, or systems that are required to continue without interruption?

   Recovery after short interruption

   Which functions, processes, or systems can be interrupted for a short time?

   Minimum Recovery Times

   Are recovery times stated?

   Standalone Units

   Does a contingency plan exist for any standalone workstation? A key part of a contingency plan should address any standalone workstations that are part of the critical operations environment. It should state where backup software and support data for these workstations is stored.

   Is the plan reviewed and approved by other key affected persons?

2. Assumptions

   Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?

3. Authority/References

   - Who or what document is authorizing the creation of the contingency plan?
   - What are the key references that apply to the plan?

4. Definition of what the Contingency Plan Addresses

   Organizations

To which organizations does the contingency plan apply?

Systems

Is there a general description of systems and/or processes?

Boundaries

5. Three phases defined

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

Respond

Is this phase adequately described so that it is understood what activities occur therein?

Is damage/impact assessment considered?

Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?

Recover

Is this phase adequately described so that it is understood what activities occur during this phase?

Restore/Reconstitute

Is this phase adequately described so that it is understood what activities occur during this phase?

6. Roles/Responsibilities Defined

Has the necessary contingency plan implementation organization been defined and the responsibilities of all those involved clearly stated with no 'gray areas'?

Will all who have a task to perform be aware of what is expected of them?

Does the contingency plan assign responsibilities for recovery? The responsibilities of key management and staff persons should be carefully described in the contingency plan, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

Does the contingency plan address critical systems and processes?

Have emergency processing priorities been established and approved by management?

Does the contingency plan specify critical data? The contingency plan should specify the critical data needed to continue critical business functions and how frequently the data is backed up.

Has a list of critical operations, data, and applications been created? In preparation for preparing the contingency plan, a list of current critical operations, data and applications should be prepared and approved by management. These are what would be needed to continue the critical business functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.

- Does the contingency plan address issues relative to pre-planned alternate locations? The contingency plan must address any potential issues relative to pre-planned alternate locations. These include:

- Insurance
- Equipment Replacement
- Phones
- Utilities
- Security

- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities should include:
  - Prioritizing operations
  - Identifying key personnel and how to reach them
  - Listing backup systems and where they are located
  - Stocking critical forms, blank check stock and supplies off-site
  - Developing reliable sources for replacing equipment on an emergency basis.
- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?
- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?
- Have temporary data storage sites and location of stored backups been identified?
- Is the frequency of file backup documented?
- Have the arrangements been made for ensuring continuing communications capabilities?
- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
- Is system, application and other key documentation maintained at the off-site location?
- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?
- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs.

These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.

- Is the contingency plan stored off-site at alternate/backup locations? Copies of the contingency plan should be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the contingency plan that are stored in a private home must be protected from inadvertent access.

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

12. Contingency Plan Maintenance
    Schedule
        Is the contingency plan annually reviewed and tested? The contingency plan should be reviewed and tested annually under conditions as close to an emergency as can be reasonably and economically simulated.
        Is there a provision for updating the contingency plan annually?
        Is the contingency plan revised after testing, depending on test results?
13. Relationships/Interfaces
    Does the contingency plan identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.
    Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?
    Is the plan compatible with plans of interacting organizations and systems?
    What internal interfaces must be considered?
    Is the plan compatible with plans of interacting organizations and systems?
    Which corporate interfaces must be considered?
    Are there special interfaces with corporate systems that must be addressed in the contingency plan?
14. Attachments
    Does the contingency plan contain appropriate attachments, as listed below?
    A. Actions for Each Phase
        Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?
    B. Procedures
        Are there detailed instructions for:
            Responding to emergencies?
            Recovering?
            Restoring operations?
        Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency should be in place.
        Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?
        Is there an implementation plan for working from home?
    C. Call Trees
        Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?
    D. Hardware Inventory
        Are there lists of all the hardware covered by the contingency plan?
    E. Software Inventory
        Are there lists of all the software covered by the contingency plan?
    F. System Descriptions
        Are all the systems covered by the contingency plan defined, including appropriate diagrams?
    G. Alternate/Backup Site Information

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

H. Assets/Resources
Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary
Has there been a realistic assessment of the nature and size of the possible threat, and of the resources most at risk?

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

K. Manual Operations

- Are manual operating procedures in place so that certain functions can be continued manually if automated support is not available soon enough?

- Manual processing procedures should exist because in the backup phase, until automated capabilities can take over the information processing, it may be necessary to use manual processing. Provisions should be made to provide this manual capability.

L. Supplies/Materials/Equipment
Is there information that describes how and where to obtain needed supplies, materials and equipment?

M. Floor Plans
Are the necessary floor plans available?

N. Maps
Are the necessary area and street maps available?

12.0 - References

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

NIST Special Pub 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.
http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11.
http://csrc.nist.gov/publications/nistpubs/800-12
HCFA Program Memorandum, Business Continuity and Contingency Plans for Millennium Change, 12 August 1998.
Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000.
Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, Section 3.6.
http://www.gao.gov/special.pubs/ail12_19_6.pdf
Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998.

http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html
Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996.
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Appendix C
An Approach to Fraud Control

Table of Contents
(Rev. 6, 12-09-05)

1.0 - Introduction

(Rev. 4, 03-05-04)

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

2.0 - Safeguards Against Employee Fraud

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

A. Screen New Employees

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

Any blatant dishonesty in the application (such as claiming qualifications and experience the applicant never had) should remove the applicant from further consideration. Check references and crosscheck them (one against the other) for consistency as well as content. Evaluate them on the basis of the contact's personal knowledge of the applicant's job-related qualifications and integrity.

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

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

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

B. Bonding

Bonding is also known as fidelity insurance and comes in all configurations; the broader the coverage, the more expensive the premium. One of the most important things you can do is to analyze the extent and conditions of coverage in relation to possible defalcations. Liability is invariably limited in some respects. For example, coverage often does not extend to external fraud; to losses not **proven** to have been caused by fraudulent acts by covered employees; to

frauds committed by employees known to have perpetrated dishonest acts previously; to frauds whose circumstances are not properly investigated; or to frauds whose alleged perpetrators are not brought to trial. Inherent in the analysis of bonding is risk analysis of fraud in relation to specific components to develop a worst-case fraud scenario in terms of dollar-loss **before** recovery through bonding.

C. Separation of Duties

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

D. Rotation of Duties

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

E. Manual Controls

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

F. Training

Training employees in their responsibilities relative to fraud in their operations is basic to prudent management. This extends beyond the employee's own activities. For example, Title 18, U.S. Code Section 4 requires anyone having knowledge of a Federal crime to report it to the FBI

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

G. Notices

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

H. Automatic Controls

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

I. Audit Routines

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

3.0 - Checklist for Medicare Fraud

(Rev. 4, 03-05-04)

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

1) Have Medicare operations been identified where fraud or complicity in fraud may be possible, e.g. initiation/approval of payments?
2) Have individuals been assigned fraud-protection responsibilities in such components, including the responsibility for reporting possible fraud and vulnerability to fraud?
3) Do individual employees at **all** levels understand that management policy relative to fraud is dismissal and prosecution?
4) Are fiscal operations regularly audited relative to fraud vulnerability?
5) Are fraudulent acts specifically mentioned in the employee's code of ethical conduct?
6) Is employee integrity specifically addressed during the hiring process, and do background investigations elicit information that would uncover an applicant's past fraudulent activity with other employers?
7) Are operations set up in such a way as to discourage **both** individual and collusive fraudulent activity?
8) Are programs/systems tested by authorized individuals with “fraudulent” input?
9) Are audit trails generated that identify employees creating inputs or making adjustments/corrections that would pinpoint responsibility for any fraudulent act?
10) Is there an effective mechanism for detection/prevention of payments being purposely misdirected to employees, relatives, or accomplices?
11) Are new or changed programs specifically reviewed for fraudulent code by those responsible for production-run approval (persons empowered to review changes but not to make changes themselves)?
12) Are controls designed to **prevent** fraud, especially in those operations where large sums could be embezzled quickly?
13) Are all error-conditions checked for fraud potential?
14) Are balancing operations done creatively so that an embezzler could not hide discrepancies?
15) Are the official activities of all employees, at all levels, subject to independent review by different reviewers (i.e., not always by the same evaluator)?
16) Does management insist on integrity at all levels?
17) Has management announced that employee's work activities will be reviewed (in unspecified ways) for both the fact and appearance of integrity?
18) Do tape/disk library controls in fact prevent tampering with files/programs for fraudulent purposes?
19) Are alternative fraud controls invoked during emergencies?
20) Are suspected frauds investigated promptly and properly and are they thoroughly documented?
21) Are fraud audits conducted both periodically and randomly?
22) Are random samples taken of claims/bill inputs and checked back to their sources?
23) Does the Personnel department check the applicant's background, employment record, references, **and** possible criminal record **before** hiring?
24) Are badges, I.D. #'s, and passwords promptly issued **and** rescinded?
25) Is off-hours work supervised, monitored, or otherwise effectively controlled?
26) Are all employees required to take their vacations and are their replacements required to check over the vacationers' past activities?
27) Are the credentials of outsiders, such as consultants and auditors, checked out?

28) Is temporary help bonded, hired from reputable agencies, and their activities restricted to the tasks to be performed? (Same principle applies to employees temporarily borrowed from non-Medicare components.)
29) Are written procedures controlled and restricted to employees currently assigned the relevant duties?
30) Are special fraud controls specified for backup operations?
31) Are incoming checks, including returned checks, handled by two or more individuals in the mailroom and are such teams switched around so that the same people are not always working together?
32) Are blank checks and automatic check-signing equipment strictly controlled with a tamper-proof numbering mechanism?
33) Is procedure/program documentation relative to the payment process treated as highly sensitive data and safeguarded when superseded?
34) Are backup files current and **securely** stored off-site?
35) Are re-runs checked for the possibility of fraud, especially duplicate payments?

Appendix D: - CMS Information Security Guidebook for Audits

(Rev. 6, 12-09-05)

1.0 - Introduction

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

This guide has been developed to aid contractors in understanding and preparing for the various types of audits and reviews, which may be performed at their locations. Its purpose is to provide additional information on site selection criteria, audit steps and objectives, documentation requirements, the types of employees that will need to be interviewed, and space and equipment requirements for CFO audits, Section 912 Reviews, SAS 70 type II audits and Penetration/EVA testing.

1.1 - CFO/EDP Audit Acts

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

1.2 - Section 912 Evaluation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

These evaluations are conducted according to procedures established by the, Office of Information Services (OIS) with input from the U.S. Department of Health and Human Services, OIG. The procedures are organized using the eight FISMA statutory areas which include: periodic risk assessments; policies and procedures based on risk assessments that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the systems development life cycle and complies with the National Institute of Standards and Technology (NIST) standards; System Security Plans; security awareness training; periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities; remedial activities, processes and reporting for deficiencies; incident detection, reporting and response, and continuity of operations for IT systems.

1.3 - SAS 70 Audits

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Statement on Auditing Standards (SAS) No. 70, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized because it represents that a service

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

1.4 - Penetration/EVA

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO's FISCAM, dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal Government domain.
For purposes of this engagement, a network vulnerability assessment is the systematic examination of an information system, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.0 - Types of Audits

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

2.1 - CFO/EDP Audit Acts

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

The purpose of these audits is to ensure that proper IT controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for Centers for Medicare and Medicaid Services (CMS). The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.
A Chief Financial Officer (CFO) Act audit is conducted under the guidelines and supervision of the U.S. GAO. The GAO requires that all such audits follow the FISCAM. FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties. The FISCAM steps may be found on the GAO Web site at www.gao.gov under the publications section.
One overall report is created for each site audited with the final report being issued by the OIG.

2.1.1 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

2.1.2 - Audit Steps and Objectives

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

Physical Access Controls

AC-1 Classify information resources according to their criticality and sensitivity.

- AC-1.1 Resource classifications and related criteria have been established.
- AC-1.2 Owners have classified resources.

AC-3 Establish physical and logical controls to prevent or detect unauthorized access.

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

Entity Wide Security Program

SP-1 Periodically assess risks.

- SP-1.1 Risks are periodically assessed.

SP-2 Document an entity wide security program plan.

- SP-2.1 A security plan is documented and approved.
- SP-2.2 The plan is kept current.

SP-3 Establish a security management structure and clearly assign security responsibilities.

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

SP-4 Implement effective security-related personnel policies.

- SP-4.1 Hiring, transfer, termination, and performance policies address security.
- SP-4.2 Employees have adequate training and expertise.

SP-5 Monitor the security program's effectiveness and make changes as needed.

- SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them.
- SP-5.2 Management ensures that corrective actions are effectively implemented.

Segregation of Duties

SD-1 Segregate incompatible duties and establish related policies.

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

SD-2 Establish access controls to enforce segregation of duties.

- SD-2.1 Physical and logical access controls have been established.
- SD-2.2 Management reviews effectiveness of control techniques.

SD-3 Control personnel activities through formal operating procedures and supervision and review.

- SD-3.1 Formal procedures guide personnel in performing their duties.
- SD-3.2 Active supervision and review are provided for all personnel.

Service Continuity

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

SC-1.1 Critical data and operations are identified and prioritized.

SC-1.2 Resources supporting critical operations are identified.

SC-1.3 Emergency processing priorities are established.

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

SC-2.1 Data and program backup procedures have been implemented.

SC-2.2 Adequate environmental controls have been implemented.

SC-2.3 Staff have been trained to respond to emergencies.

SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.

SC-3 Develop and document a comprehensive contingency plan.

SC-3.1 An up-to-date contingency plan is documented.

SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.

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

SC-4.1 The plan is periodically tested.

SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.

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

<u>Access Controls</u>

AC-2 Maintain a current list of authorized users and their access authorized.

AC-2.1 Resource owners have identified authorized users and their access authorized.

AC-2.2 Emergency and temporary access authorization is controlled.

AC-2.3 Owners determine disposition and sharing of data.

AC-3 Establish physical and logical controls to prevent or detect unauthorized access.

AC-3.2. Adequate logical access controls have been implemented. (see also EVA)

AC-3.2.A Passwords, tokens, or other devices are used to identify and authenticate users.

AC-3.2.B Identification of access paths.

AC-3.2.C Logical controls over data files and software programs.

AC-3.2.D Logical controls over a database.

AC-3.2.E Logical controls over telecommunications access.

AC-3.3 Cryptographic tools. (see also EVA)

AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.

AC-4.1 Audit trails are maintained.

AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.

AC-4.3 Suspicious access activity is investigated and appropriate action is taken.

<u>Application Software Development and Change Control</u>

CC-1 Processing features and program modifications are properly authorized.

CC-1.1 A system development life cycle methodology (SDLC) has been implemented.

CC-1.2 Authorizations for software modifications are documented and maintained,

CC-1.3 Use of public domain and person software is restricted.

CC-2 Test and approve all new and revised software.

CC-2.1 Changes are controlled as programs progress through testing to final approval.

CC-2.2 Emergency changes are promptly tested and approved.

CC-2.3 Distribution and implementation of new or revised software is controlled,

CC-3 Control software libraries

CC-3.1 Programs are labeled and inventoried.

CC-3.2 Access to program libraries is restricted.

CC-3.3 Movement of programs and data among libraries is controlled.

Systems Software

SS-1 Limit access to systems software.

SS-1.1 Access authorizations are appropriately limited.

SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths.

SS-2 Monitor access to and use of systems software.

SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.

SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.

SS-3 Control systems software changes.

SS-3.1 Systems software changes are authorized, tested, and approved before implementation.

SS-3.2 Installation of systems software is documented and reviewed.

2.1.3 - Testing Procedures

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Please refer to Table 2 in Section 3.0 of this appendix for detailed testing procedures.

2.1.4 - Documentation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

1. Entity-wide security programs (e.g., System Security Plan).
2. Network diagrams.
3. Risk assessments and vulnerability analyses.
4. Organizational charts which include names and titles for the Medicare, information systems, and information system security departments.
5. Completed Core Set of Security Requirements using the CMS Integrated Security Suite (CISS, formerly the Contractor Assessment Security Tool, a.k.a. "CAST").
6. Risk Assessment policies and any internal risk analysis documentation
7. Documentation on data and resource classification
8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
9. The most recent SAS 70 and risk assessment reports
10. Policies and procedures regarding conduct in the data center
11. Policies and procedures for back-up tape rotation and off-site storage
12. Policies and procedures for sanitation of media prior to disposal
13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
15. Layout of company buildings and overview of operations in each building

16. Employee lists for Medicare, information systems, and information system security departments (lists should include: name or identification (ID) number, job title, department, start date, and position effective date)
17. Documentation of new hire/information system security training program
18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas
19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract
20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.
21. Policies and procedures regarding the testing of the plan
22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable
23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

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

<u>Logical Access Controls</u>

Information on logical access controls, including the following:

NOTE: Detailed reports will vary based on security software in use, i.e., RACF, Top Secret, ACF2, UNIX, NT, etc.

1. Security policies, standards, and procedures for:
    a. Creation, modification, and deletion of user-IDs, functional groups, etc.
    b. Periodic review of access
    c. Dial-up access
    d. Use and monitoring of emergency or temporary access (Fire-call IDs)
    e. Password composition/mask
    f. Violation and security monitoring
    g. Archiving, deleting, or sharing data files
    h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)
2. List of all terminations during the current fiscal year
3. List of all transfers during the current fiscal year
4. List of all new hires during the current fiscal year
5. List of all Medicare application users
6. List of all users with dial up access
7. List of all users with the ability to change security settings (administrators)
8. Access to access requests and authorizations (for a sample of users)
9. List of access request approvers
10. Documentation supporting recertification of users
11. List of emergency or temporary (fire-call) IDs
12. Activity log of emergency or temporary IDs
13. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties
14. System default password requirements

15. Use of generic, group or system IDs
16. Database security requirements and settings
17. Security violation logging and monitoring
18. Evidence of review of user templates and/or profiles
19. Evidence of automatic timeout on terminals
20. Database access lists
21. Evidence supporting resolution of prior year audit findings

Systems Software

Systems Software information including:

1. Results of CA_EXAMINE runs
2. Policies and procedures for restricting access to systems software
3. A list of all system programmers
4. A list of all application programmers
5. A list of all computer operators
6. Results of the last review of system programmer access capabilities
7. A list of all vendor supplied software that indicates how current the software is
8. If available, integrity statements from vendors for all third party software
9. Policies and procedures for using and monitoring use of system utilities
10. Policies and procedures for identifying, selecting, installing and modifying systems software
11. Policies and procedures for disabling vender supplied defaults
12. Roles and responsibilities for system programmers
13. Policies and procedures for emergency software changes

- 14. A list of all systems software changes made during the fiscal year

15. A list of all emergency changes made during the fiscal year
16. A list of all current access to systems software
17. A list of all users with access to migrate programs to production
18. A sample of audit logs for system utilities and system programmer activity
19. Evidence of review of logs and follow up action taken
20. Initial Program Load (IPL) procedures
21. Log from last IPL

Application Development and Change Management

Information on change management, including the following:

1. System Development Life Cycle (SDLC) methodology document
2. A list of all changes made during the current fiscal year
3. Dates of and training materials from the most
4. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
5. A list of all authorized change request approvers
6. Policies and procedures over the use of personal and public domain software:
7. Test plan standards
8. A log of ABENDS
9. Procedures for new software distribution
10. Policies and procedures for emergency changes
11. A list of all emergency changes during the current fiscal year
12. Identification of virus software in use

- 13. A list of all users with access to library management software

14. A list of all users with access to the production libraries (production code, source code, extra program copies)
15. Tape library logs for the most recent 3 months

2.1.5 - Interviews Required

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

2.1.6 - Space and Equipment Requirements

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

2.2 - Section 912 Evaluation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

The CMS-contracted auditor has agreed to perform procedures established by CMS OIS and the U.S. Department of Health and Human Services, Office of Inspector General (OIG) associated with the eight FISMA statutory areas which include: Periodic risk assessments; Policies and

procedures based on risk assessments that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the systems development life cycle and complies with the NIST standards; System Security Plans; Security awareness training; Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities; Remedial activities, processes and reporting for deficiencies; Incident detection, reporting and response; and, Continuity of operations for IT systems.

2.2.1 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

2.2.2 - Audit Steps and Objectives

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Risk Assessments

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

Policies and procedures to reduce risk

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

Review of System Security Plans

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

Review of security awareness training

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

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

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

Review of remedial activities, processes and reporting for deficiencies

1. Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses
2. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.

3. Determine the number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.

Review of incident detection, reporting and response

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

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

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

2.2.3 - Testing Procedures

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Please refer to Table 3 in section 3.0 of this appendix for detailed testing procedures.

2.2.4 - Documentation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

Risk Assessment Review

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

Policies & Procedures

1. IT Security
2. Job descriptions for management

System Security Plan

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

Review of Security Awareness Training

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

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

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

Review of remedial activities, processed and reporting for deficiencies

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

Review of incident detection, reporting and response

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

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

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

2.2.5 - Interviews Required

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

1. Medicare compliance officer
2. Person responsible for the CAP
3. Person responsible for IT Risk Assessment
4. Person responsible for the System Security Plan
5. Person in charge of training (entity wide security program)
6. Internal audit lead
7. HR contact
8. Mainframe systems administrator
9. Mainframe security administrator
10. LAN administrator
11. LAN security officer

12. Security software administrator
13. Systems programming manager
14. Person in charge of maintaining the System and Business Continuity Plan
15. Person in charge of the data center
16. Manager of physical security
17. Head of computer operations
18. Person in charge of change management
19. Application manager for the following systems:
    a. FISS
    b. MCS
    c. VMS

2.2.6 - Space and Equipment Requirements

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

2.3 - SAS 70 Audits

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

2.3.1 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

2.3.2 - Audit Steps and Objectives

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

Entity-wide Security Program

Access Controls

Control of Application Development and Implementation

Systems Software
Service Continuity
Segregation of Duties

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

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

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

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

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

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

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

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

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

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

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

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

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

A.13 A regular risk assessment of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats,

known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.

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

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

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

A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components and operations.

A.18 Management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.

A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts and actual intrusions.

A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with the Federal Information Security Management Act (FISMA)

2.3.3 - Testing Procedures

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

Please refer to Table 4 in section 3.0 of this appendix for detailed testing procedures.

2.3.4 - Documentation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

1. Entity wide security programs (e.g., System Security Plan)
2. Network diagrams
3. Risk assessments and vulnerability analyses
4. Organizational charts that include names and titles for the Medicare, information systems, and information system security departments
5. Completed CSRs using the CISS
6. Risk Assessment policies and any internal risk analysis documentation
7. Documentation on data and resource classification
8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
9. The most recent SAS 70 and risk assessment reports
10. Policies and procedures regarding conduct in the data center
11. Policies and procedures for back-up tape rotation and off-site storage
12. Policies and procedures for sanitation of media prior to disposal
13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
15. Layout of company buildings and overview of operations in each building

16. Employee lists for Medicare, information systems, and information system security departments (lists should include: name or identification (ID) #, job title, department, start date, and position effective date)
17. Documentation of new hire/information system security training program
18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas
19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract
20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.
21. Policies and procedures regarding the testing of the plan
22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable
23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan
24. Security policies, standards, and procedures for:
    a. Creation, modification, and deletion of user-IDs, functional groups, etc.
    b. Periodic review of access
    c. Dial-up access
    d. Use and monitoring of emergency or temporary access (Fire-call IDs)
    e. Password composition/mask
    f. Violation and security monitoring
    g. Archiving, deleting, or sharing data files
    h. Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)
25. List of all terminations during the current fiscal year
26. List of all transfers during the current fiscal year
27. List of all new hires during the current fiscal year
28. List of all Medicare application users
29. List of all users with dial up access
30. List of all users with the ability to change security settings (administrators)
31. Access to access requests and authorizations (for a sample of users)
32. List of access request approvers
33. Documentation supporting recertification of users
34. List of emergency or temporary (fire-call) IDs
35. Activity log of emergency or temporary IDs
36. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties
37. System default password requirements
38. Use of generic, group or system IDs
39. Database security requirements and settings
40. Security violation logging and monitoring
41. Evidence of review of user templates and/or profiles
42. Evidence of automatic timeout on terminals
43. Database access lists
44. Evidence supporting resolution of prior year audit findings

45. Results of CA_EXAMINE runs
46. Policies and procedures for restricting access to systems software
47. A list of all system programmers
48. A list of all application programmers
49. A list of all computer operators
50. Results of the last review of system programmer access capabilities
51. A list of all vendor supplied software indicating the current version of the software
52. If available, integrity statements from vendors for all third party software
53. Policies and procedures for using and monitoring use of system utilities
54. Policies and procedures for identifying, selecting, installing and modifying systems software
55. Policies and procedures for disabling vender supplied defaults
56. Roles and responsibilities for system programmers
57. Policies and procedures for emergency software changes
58. A list of all systems software changes made during the fiscal year
59. A list of all emergency changes made during the fiscal year
60. A list of all current access to systems software
61. A list of all users with access to migrate programs to production
62. A sample of audit logs for system utilities and system programmer activity
63. Evidence of review of logs and follow up action taken
64. Initial Program Load (IPL) procedures
65. Log from last IPL
66. System Development Life Cycle (SDLC) methodology document
67. Change control policies and procedures (if not included in the SDLC document)
68. A list of all changes made during the current fiscal year
69. Dates of and training materials from the most recent SDLC training class
70. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
71. A list of all authorized change request approvers
72. Policies and procedures over the use of personal and public domain software:
73. Test plan standards
74. A log of abends
75. Procedures for new software distribution
76. Policies and procedures for emergency changes
77. A list of all emergency changes during the current fiscal year
78. Identification of virus software in use
79. A list of all users with access to library management software
80. A list of all users with access to the production libraries (production code, source code, extra program copies)
81. Tape library logs for the most recent 3 months
82. Current system configurations documentation including links to other systems
83. Threat source documentation (manmade/natural)
84. Documented system vulnerabilities, system flaws or weaknesses
85. Mission/business impact analysis
86. Job descriptions for management
87. Information security job responsibilities

88. Background check policies/procedures
89. Security policy/procedure updates
90. Management review of corrective actions
91. Training/professional development policies/procedures
92. Training schedule (if applicable)
93. Awareness posters, booklets, newsletters, etc
94. Management reports for review & testing of IT security policies & procedures
95. Independent audit reports and evaluations
96. Tracking of weaknesses (DB, paper, etc)
97. Planned corrective actions
98. CAP
99. List of IT security weaknesses including dates of corrective actions
100. Policies/procedures for monitoring systems & the network
101. Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions

2.3.5 - Interviews Required

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

2.3.6 - Space and Equipment Requirements

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

3. Access to copier, fax machine, and printer.

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

2.4 - Penetration/EVA

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

2.4.1 - Execution of the Audit

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

The CMS-contracted auditor is the Independent Public Accountant (IPA) engaged by the OIG Department of Health and Human Services (HHS) to perform testing at third party CMS contractors as part of the FY 2004 Financial Statement Audit of the Centers for Medicare and Medicaid Services ("CMS").

There will be a site summary that includes a high level description of the testing performed and findings describing technical issues identified during testing. The findings will be written in terms of Condition, Cause, Criteria, Effect, and Recommendation (following GAO Yellow Book guidelines). The Site Summary will be supported by summary work papers for each type of testing performed.

2.4.2 - Site Selection Criteria

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

2.4.3 - Audit Steps and Objectives

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

<u>Steps to perform penetration testing</u>

<u>Phase 1 – Assess & Model Threats</u>

The Assess & Model Threats phase is used to establish and acquire the information required to successfully define the scope of the security penetration testing. This involves gathering information and completing an initial threat analysis to ensure that testing emulates the threats

that are of real concern to the organization. This includes project start-up, information gathering and threat analysis.

1. Threat analysis is usually conducted according to prescribed scenarios that are clearly documented in the Statement of Work. Some common threat scenarios for an external penetration test include:

    a. Untrusted Outsider – This is the most common scenario for an External (Internet) penetration test. This scenario is designed to simulate individuals with no significant knowledge of the client's computing operations that are attempting to gain access from remote locations;

    b. Trusted Outsider – This scenario is designed to simulate third parties (e.g., customers, suppliers, partners) that have limited legitimate access to the client's network. In the event of the trusted outsider scenario, establish with the client what resources the team will attack and arrange for the client to set up valid credentials to access those resources (e.g., usernames/passwords, SecurID tokens).

2. During the project start-up, agree on primary contacts for both the CMS-contracted auditor and the client to contact in case of an emergency. These contact numbers should be accessible at all times during testing. All members of the team should be aware of the escalation path and procedures during testing.
3. Determine with the client when testing should stop. Some clients request that as soon as access is obtained, the CMS-contracted auditor stop and notify the client before attempting to obtain further access to resources.
4. Determine if there are specific targets of interest that the CMS-contracted auditor should direct attacks to (e.g., a focus on the client's web server).
5. All penetration activities must be conducted from either a CMS-contracted auditor lab or the client site. Identify the source IP range you will be using with the client to allow them to differentiate the CMS-contracted auditor activities from legitimate hacking attempts. Contact your lab manager for information on your external IP address range.
6. Establish acceptable timeframes for penetration testing with the client to avoid disrupting day-to-day client business (and to avoid being caught if the engagement requires stealth testing).
7. Inquire about any IP addresses that should be excluded from testing.

<u>Phase 2 – Survey Testing</u>

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

1. Identify Internet connections and IP ranges by querying public databases.
2. Identify salient target information available in newsgroups and web pages.
3. Use DNS queries to identify client networks and systems. These queries are best performed from a UNIX system that has the dig utility installed (NOTE: dig is also available for Windows systems). IP addresses that are found through DNS queries should be looked up in the Internet repositories listed above to determine the range and owner of the IP address. The following queries can be used to identify client systems and networks:
4. Once you have identified client IP ranges and accessible websites, confirm IP addresses with the client contact before attempting to attack any systems.

a. Once the client has approved the IP ranges identified during the first part of this phase, scans can be conducted using a map to identify open ports and potential attack points on each of the servers in the range. Depending on the requirements of the organization, different types of scans may be used to try and avoid detection.

5. Once the initial scan is complete, a table should be created for the information gathered from each port.
6. After you have identified the services running on each port and obtained all information possible, the Intrusion Testing Phase of the engagement can begin. Note: confirm with the engagement manager before beginning Intrusion testing to determine if the client needs to be notified before beginning.

Phase 3 – Intrusion Testing

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

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

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

Phase 4 – Assess Exposures

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

2.4.4 - Documentation

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

Additional Penetration/EVA items include:

1. Personnel to observe the penetration and diagnostic testing activities (if desired by the auditee).
2. Permission to connect the CMS-contracted auditor laptop to site's network (while monitored).
3. Network access for internal testing.

System administrator/programmer access for systems to perform diagnostic review.

- 4. Specific documents required by the CMS-contracted auditor will be requested in the Provided by Client (PBC) list. This list will be provided prior to the start of testing.

2.4.5 - Interviews Required

(Rev.6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

2.4.6 - Space and Equipment Requirements

(Rev.6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

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

3.0 - Tables

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

TABLE 1: SYNOPSIS OF DOCUMENTATION REQUIRED

This chart provides a synopsis of required documentation.

Documentation	CFO Audit	Section 912	SAS 70	EVA
Entity wide security programs (e.g., System Security Plan).	✔	✔	✔	
Network diagrams.	✔	✔	✔	✔
Risk assessments and vulnerability analyses.	✔	✔	✔	
Organizational charts which include names and titles for the Medicare, information systems, and information system security departments.	✔	✔	✔	
Completed CSRs using the CISS	✔	✔	✔	
Risk Assessment policies and any internal risk analysis documentation.	✔	✔	✔	
Documentation on data and resource classification.	✔	✔	✔	
HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations.	✔	✔	✔	
The most recent SAS 70 and risk assessment reports.	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EV A
Policies and procedures regarding conduct in the data center.	✔		✔	
Policies and procedures for back-up tape rotation and off-site storage	✔	✔	✔	
Policies and procedures for sanitation of media prior to disposal	✔	✔	✔	
Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms.	✔		✔	
Policies and procedures regarding visitors to both the general campus and to the sensitive areas.	✔		✔	
Layout of company buildings and overview of operations in each building.	✔		✔	
Employee lists for Medicare, information systems, and information system security departments (lists should include: name or identification (ID) #, job title, department, start date, and position effective date).	✔	✔	✔	
Documentation of new hire/information system security training program.	✔	✔	✔	
Vendor sign in and sign out logs for maintenance or repairs in sensitive areas.	✔		✔	
Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract.	✔		✔	
Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.	✔	✔	✔	
Policies and procedures regarding the testing of the plan.	✔	✔	✔	
Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable.	✔	✔	✔	
Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan.	✔	✔	✔	
Security policies, standards, and procedures for:				
Creation, modification, and deletion of user-IDs, functional groups, etc.	✔		✔	
Periodic review of access.	✔		✔	
Dial-up access.	✔		✔	
Use and monitoring of emergency or temporary access (Fire-call IDs).	✔		✔	
Password composition/mask.	✔		✔	✔

Documentation	CFO Audit	Section 912	SAS 70	EV A
Violation and security monitoring.	✔		✔	
Archiving, deleting, or sharing data files.	✔		✔	
Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.).	✔		✔	
List of all terminations during the current fiscal year.	✔		✔	
List of all transfers during the current fiscal year.	✔		✔	
List of all new hires during the current fiscal year.	✔		✔	
List of all Medicare application users.	✔	✔	✔	
List of all users with dial up access.	✔		✔	
List of all users with the ability to change security settings (administrators).	✔		✔	
Access to access requests and authorizations (for a sample of users).	✔		✔	
List of access request approvers.	✔		✔	
Documentation supporting recertification of users.	✔		✔	
List of emergency or temporary (fire-call) IDs.	✔		✔	
Activity log of emergency or temporary IDs.	✔		✔	
Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties.	✔		✔	
System default password requirements.	✔		✔	
Use of generic, group or system IDs.	✔		✔	
Database security requirements and settings.	✔		✔	
Security violation logging and monitoring.	✔		✔	
Evidence of review of user templates and/or profiles.	✔		✔	
Evidence of automatic timeout on terminals.	✔		✔	
Database access lists.	✔		✔	
Evidence supporting resolution of prior year audit findings.	✔		✔	
Results of CA_EXAMINE runs.	✔		✔	
Policies and procedures for restricting access to systems software.	✔		✔	
A list of all system programmers.	✔		✔	
A list of all application programmers.	✔		✔	
A list of all computer operators.	✔		✔	
Results of the last review of system programmer access capabilities.	✔		✔	
A list of all vendor supplied software that indicates how current the software is.	✔		✔	
If available, integrity statements from vendors for all third party software.	✔		✔	
Policies and procedures for using and monitoring use of system utilities.	✔		✔	
Policies and procedures for identifying, selecting,	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EV A
installing and modifying systems software.				
Policies and procedures for disabling vender supplied defaults.	✔		✔	
Roles and responsibilities for system programmers.	✔		✔	✔
Policies and procedures for emergency software changes.	✔		✔	
A list of all systems software changes made during the fiscal year	✔		✔	
A list of all emergency changes made during the fiscal year.	✔		✔	
A list of all current access to systems software.	✔		✔	
A list of all users with access to migrate programs to production.	✔		✔	
A sample of audit logs for system utilities and system programmer activity.	✔		✔	
Evidence of review of logs and follow up action taken.	✔		✔	
Initial Program Load (IPL) procedures.	✔		✔	
Log from last IPL.	✔		✔	
System Development Life Cycle (SDLC) methodology document.	✔	✔	✔	
Change control policies and procedures (if not included in the SDLC document).	✔		✔	
A list of all changes made during the current fiscal year.	✔		✔	
Dates of and training materials from the most recent SDLC training class.	✔		✔	
Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork).	✔		✔	
A list of all authorized change request approvers.	✔		✔	
Policies and procedures over the use of personal and public domain software:	✔		✔	
Test plan standards.	✔		✔	
A log of ABENDS.	✔		✔	
Procedures for new software distribution.	✔		✔	
Policies and procedures for emergency changes	✔		✔	
A list of all emergency changes during the current fiscal year.	✔		✔	
Identification of virus software in use.	✔		✔	
A list of all users with access to library management software.	✔		✔	
A list of all users with access to the production	✔		✔	

Documentation	CFO Audit	Section 912	SAS 70	EV A
libraries (production code, source code, extra program copies).				
Tape library logs for the most recent 3 months.	✔		✔	
Current system configurations documentation including links to other systems.		✔	✔	
Threat source documentation (manmade/natural).		✔	✔	
Documented system vulnerabilities, system flaws or weaknesses.		✔	✔	
Mission/business impact analysis		✔	✔	
Job descriptions for management		✔	✔	
Information security job responsibilities.		✔	✔	
Background check policies/procedures.		✔	✔	
Security policy/procedure updates.		✔	✔	
Management review of corrective actions		✔	✔	
Training/professional development policies/procedures		✔	✔	
Training schedule (if applicable).		✔	✔	
Awareness posters, booklets, newsletters, etc.		✔	✔	
Management reports for review & testing of IT security policies & procedures.		✔	✔	
Independent audit reports and evaluations.		✔	✔	
Tracking of weaknesses (DB, paper, etc).		✔	✔	
Planned corrective actions.		✔	✔	
All four quarter CAPs.		✔	✔	
List of IT security weaknesses including dates of corrective actions.		✔	✔	
Policies/procedures for monitoring systems & the network.		✔	✔	
Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions.		✔	✔	
Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.				✔
Standards and Guidelines (Risk Model) for system configuration.				✔
Applicable phone number range for dial-up “war-dialing” testing.				✔
Applicable Internet Protocol (IP) address spaces for penetration testing.				✔
Listing of IP addresses assigned to, or under the purview of the site.				✔
Listing of prohibited telephones/systems/networks.				✔

TABLE 2: DETAILED CFO TESTING PROCEDURES

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

	4. Review documentation on and logs of entry code changes.
	5. Observe appointment and verification procedures for visitors.
2. Sanitation of equipment and media prior to disposal or reuse.	1. Review written procedures.
	2. Interview personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software.
	4. For selected items still in the entity's possession, test that they have been appropriately sanitized.
Entity Wide Security Program	
SP-1 Risks are periodically assessed.	
1. Risks are periodically assessed.	1. Review risk assessment policies.
	2. Review the most recent high-level risk assessment.
	3. Review the objectivity of personnel who performed and reviewed the assessment.
SP-2 Document an entitywide security program plan.	
1. A security plan is documented and approved.	1. Review the security plan.
	2. Determine whether the plan covers the topics prescribed by OMB Circular A-130.
2. The plan is kept current.	1. Review the security plan and any related documentation indicating that it has been reviewed and updated and is current.
SP-3 Establish a security management structure and clearly assign security responsibilities.	
1. A security management structure has been established.	1. Review the security plan and the entity's organization chart.
	2. Interview security management staff.
	3. Review pertinent organization charts and job descriptions.
	4. Interview the security manager.
2. Information security responsibilities are clearly assigned.	1. Review the security plan.
3. Owners and users are aware of security policies.	1. Review documentation supporting or evaluating the awareness program. Observe a security briefing.
	2. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
	3. Review memos, electronic mail files, or other policy distribution mechanisms.
	4. Review personnel files to test whether security awareness statements are current.

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

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

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

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

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

	3. Review any documentation supporting contingency plan adjustments.

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

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

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

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

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

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

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

	10. Test for default presence using vendor standard IDs and passwords.
	11. Determine what terminals are set up as master consoles and what controls exist over them.
	12. Test to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
SS-2 Monitor access to and use of systems software.	
1. Policies and techniques have been implemented for using and monitoring use of system utilities.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel regarding their responsibilities.
	3. Determine whether logging occurs and what information is logged.
	4. Review logs.
	5. Using security software reports, determine who can access the logging files.
2. Inappropriate or unusual activity is investigated and appropriate actions taken.	1. Interview technical management regarding their reviews of privileged systems software and utilities usage.
	2. Review documentation supporting their reviews.
	3. Interview management and systems personnel regarding these investigations.
	4. Review documentation supporting these investigations.
	5. Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff.
	6. Review documentation supporting their supervising and monitoring of systems programmers' activities.
	7. Interview management and analyze their reviews concerning the use of systems software.
	8. Determine what management reviews have been conducted, and their currency, over this area.
SS-3 Control systems software changes.	
1. Systems software changes are authorized, tested, and approved before implementation.	1. Review pertinent policies and procedures.
	2. Interview management and systems personnel.
	3. Review procedures for identifying and documenting systems software problems.
	4. Interview management and systems programmers.
	5. Review the causes and frequency of any recurring systems software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	6. Determine what authorizations and documentation are required prior to initiating systems software changes.

	7. Select recent systems software changes and determine whether the authorization was obtained and the change is supported by a change request document.
	8. Determine the procedures used to test and approve systems software prior to its implementation.
	9. Select recent systems software changes and test whether the indicated procedures were in fact used.
	10. Review procedures used to control and approve emergency changes.
	11. Select some emergency changes to systems software and test whether the indicated procedures were in fact used.
2. Installation of systems software is documented and reviewed.	1. Interview management and systems programmers about scheduling and giving advance notices when systems software is installed.
	2. Review recent installations and determine whether scheduling and advance notification did occur.
	3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
	4. Interview management, systems programmers, and library control personnel, and determine who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries.
	5. Review supporting documentation for some systems software migrations and the removal of outdated versions from production libraries.
	6. Interview data center management about their role in reviewing systems software installations.
	7. Review some recent systems software installations and determine whether documentation shows that logging and management review occurred.
	8. Interview systems software personnel concerning a selection of systems software and determine the extent to which the operating version of the systems software is currently supported by the vendor.
	9. Interview management and systems programmers about the currency of systems software and the currency and completeness of software documentation.
	10. Review documentation and test whether recent changes are incorporated.

TABLE 3: DETAILED MMA 912 TESTING PROCEDURES

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

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

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

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

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

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

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

TABLE 4: DETAILED SAS 70 TESTING PROCEDURES

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

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

11. Employees have received a copy of or have easy access to agency security procedures and policies.	1. Inquired of appropriate personnel regarding employee access to agency security procedures and policies.
	2. Inspected evidence that employees have received a copy or have easy access to the agency security procedures and policies.
	3. Reviewed policies and procedures in which employees have easy access to ensure that they are the most current.
12. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.	1. Identified all employees responsible for administering security.
	2. Reviewed training records and certifications for all security employees to ensure that adequate training has been received.
	3. Inquired of appropriate personnel regarding the documentation and tracking of application specific training for employees.
	4. Reviewed the most recent application specific training curriculum.
	5. Inspected evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual and temporary) and include termination and transfer procedures that require exit interviews, return of property, such as keys and ID cards, notification to security management of terminations, removal of access to systems and escorting of terminated employees out of the facility.	
1. Hiring, transfer, termination, and performance policies address security.	1. Reviewed hiring policies and procedure to ensure that they address security.
	2. Reviewed transfer policies and procedures to ensure that they address security.
	3. Reviewed termination policies and procedures to ensure that they address security.
	4. Ensured that performance policies and procedures (i.e., Rules of Behavior and Performance Evaluations) address security.
	5. Reviewed reinvestigation policies.
	6. Reviewed policies and procedures for performing background checks.
	7. For a selection of sensitive positions, inspected personnel records and determined whether background reinvestigations have been performed.

	8. Reviewed policies on confidentiality or security agreements.
	9. For a selection of such users, determined whether confidentiality or security agreements are on file.
	10. Reviewed vacation policies.
	11. Inspected personnel records to identify individuals who have not taken vacation or sick leave in the past year.
	12. Determined who performed vacationing employee's work during vacation.
	13. Reviewed job rotation policies.
	14. Reviewed staff assignment records and determined whether job and shift rotations occur.
	15. Reviewed pertinent policies and procedures.
	16. For a selection of terminated or transferred employees, examined documentation showing compliance with policies.
	17. Compared a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.
2. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
3. Employees have received a copy of the Rules of Behavior.	1. Inquired of the appropriate personnel regarding the maintenance and distribution of the Rules of Behavior for all types of employees.
	2. Reviewed the most current version of the Rules of Behavior.
	3. Selected a sample of employees and ensured that they have received a copy of the most current version of the rules of behavior.
A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.	
1. Resource classifications and related criteria have been established.	1. Reviewed data classification policies and procedures.
	2. Interviewed resource owners.
2. Owners have classified resources.	1. Reviewed resource classification documentation and compared to risk assessments. Discussed any discrepancies with appropriate officials.

3. Data sensitivity and integrity have been documented and data has been classified.	1. Reviewed evidence based on policies and procedures that data has been classified.
A.4 Access to computerized applications, systems software, and Medicare data is appropriately authorized, documented, and monitored, and includes approval by resource owners, procedures to control emergency and temporary access, and procedures to share and properly dispose of data.	
1. Resource owners have identified authorized users and their access authorized.	1. Reviewed pertinent written policies and procedures.
	2. For a selection of users (both application user and information security personnel) reviewed access authorization documentation.
	3. Interviewed owners and reviewed supporting documentation. Determined whether inappropriate access is removed in a timely manner.
	4. For a selection of users with dial-up access, reviewed authorization and justification.
	5. Interviewed security managers and reviewed documentation provided to them.
	6. Reviewed a selection of recent profile changes and activity logs.
	7. Obtained a list of recently terminated employees from Personnel and, for a selection, determined whether system access was promptly terminated.
2. Emergency and temporary access authorization is controlled.	1. Reviewed pertinent policies and procedures.
	2. Compared a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.
	3. Determined the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
3. Owners determine disposition and sharing of data.	1. Examined standard approval forms.
	2. Interviewed data owners.
	3. Examined documents authorizing file sharing and file sharing agreements.
4. Sanitation of equipment and media prior to disposal or reuse.	1. Reviewed written procedures.
	2. Interviewed personnel responsible for clearing equipment and media.
	3. For a selection of recently discarded or transferred items, examined documentation related to clearing of data and software.

	4. For selected items still in the entity's possession, tested that they have been appropriately sanitized.
5. Access authorizations are appropriately limited.	1. Reviewed policies and procedures regarding the disposal of data and equipment to ensure that applicable Federal security and privacy requirements are included.
	2. Interviewed management and systems personnel regarding access restrictions.
	3. Observed personnel accessing systems software, such as sensitive utilities, and noted the controls encountered to gain access.
	4. Attempted to access the operating system and other systems software.
	5. Selected some systems programmers and determined whether management-approved documentation supports their access to systems software.
	6. Selected some application programmers and determined whether they are not authorized access.
	7. Determined the last time the access capabilities of system programmers were reviewed.
6. Passwords, tokens, or other devices are used to identify and authenticate users.	1. Reviewed pertinent policies and procedures.
	2. Reviewed security software password parameters.
	3. Observed users keying in passwords.
	4. Attempted to log on without a valid password; make repeated attempts to guess passwords.
	5. Assessed procedures for generating and communicating passwords to users.
	6. Reviewed a system-generated list of current passwords.
	7. Searched password file using audit software.
	8. Attempted to log on using common vendor supplied passwords.
	9. Interviewed users and security managers.
	10. Reviewed a list of IDs and passwords.
	11. Repeatedly attempted to log on using invalid passwords.
	12. Reviewed security logs.
	13. Reviewed pertinent policies and procedures.
	14. Reviewed documentation of such comparisons.
	15. Interviewed security managers.
	16. Made comparison using audit software.
	17. Viewed dump of password files (e.g., hexadecimal printout).

	18. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor obtained the assistance of a specialist.
7. Identification of access paths.	1. Reviewed access path diagram.
8. Logical controls over data files and software programs.	1. Interviewed security administrators and system users.
	2. Reviewed security software parameters.
	3. Observed terminals in use.
	4. Reviewed a system-generated list of inactive logon IDs, and determined why access for these users has not been terminated.
	5. Determined library names for sensitive or critical files and libraries and obtained security reports of related access rules. Using these reports, determined who has access to critical files and libraries and whether the access matches the level and type of access authorized.
	6. Performed penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system.
	7. When performing outsider tests, tested the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
	8. When performing insider tests, used an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, tried to access the entity's computer resources using default/generic IDs with easily guessed passwords.
	9. Determined whether naming conventions are used.
9. Logical controls over a database.	1. Reviewed pertinent policies and procedures.
	2. Interviewed database administrator.
	3. Reviewed DBMS and DD security parameters.
	4. Tested controls by attempting to access restricted files.
	5. Reviewed security system parameters.
10. Logical controls over telecommunications access.	1. Reviewed pertinent policies and procedures.
	2. Reviewed parameters set by communications software or teleprocessing monitors.
	3. Tested telecommunications controls by attempting to access various files through communications networks.
	4. Identified all dial-up lines through automatic dialer software routines and compared with known dial-up access. Discussed discrepancies with management.

	5. Interviewed telecommunications management staff and users.
	6. Reviewed pertinent policies and procedures.
	7. Viewed the opening screen seen by telecommunication system users.
	8. Reviewed the documentation showing changes to dial-in numbers.
	9. Reviewed entity's telephone directory to verify that the numbers are not listed.
11. Cryptographic tools	1. To evaluate cryptographic tools, the auditor obtained the assistance of a specialist.
A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.	
1. All access paths have been identified and controls implemented to prevent or detect access for all paths.	1. Tested the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.
	2. Obtained a list of vendor-supplied software and determined if any of these products have known deficiencies that adversely impact the operating system integrity controls.
	3. Judgmentally reviewed the installation of systems software components and determined whether they were appropriately installed to preclude adversely impacting operating system integrity controls.
	4. Performed an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods.
	5. Obtained a list of all systems software on test and production libraries used by the entity.
	6. Verified that access control software restricts access to systems software.
	7. Using security software reports, determined who has access to systems software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated In the presence of the auditor.
	8. Verified that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	9. Inquired whether disabling has occurred.
	10. Tested for default presence using vendor standard IDs and passwords.

	11. Determined what terminals are set up as master consoles and what controls exist over them.
	12. Tested to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.
2. Security policies and procedures include controls to address platform security configurations, and patch management.	1. Reviewed platform security configuration policies and procedures.
	2. Reviewed patch management policies and procedures.
3. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
A.6 Physical access by all employees, including visitors, to Medicare facilities, data centers and systems is appropriately authorized, documented, and access violations are monitored and investigated.	
1. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	1. Reviewed a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.
	2. Performed a walkthrough of data center to ensure that adequate physical security controls exist.
	3. Reviewed lists of individuals authorized access to sensitive areas and determined the appropriateness for access.
	4. Before becoming recognized as the auditor, attempted to access sensitive areas without escort or identification badges.
	5. Observed entries to and exits from facilities during and after normal business hours.
	6. Observed utilities access paths.
	7. Inquired of data center manager concerning the physical security controls implemented in the data center.
	8. Observed entries to and exits from sensitive areas during and after normal business hours.
	9. Reviewed procedures for the removal and return of storage media from and to the library.

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

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

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

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

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

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

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

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

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

5. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	1. Reviewed the most current risk assessment.
	2. Reviewed IT Security policies and procedures to ensure that they reduce the risk outlined in the risk assessment.
	3. Ensured that IT Security policies and procedures are current.
6. Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1. Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures.
	2. Reviewed documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
7. Management reports for the review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspected evidence that periodic testing of IT security policies and procedures (including network risk assessments, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.
8. Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
A.15 A Risk Assessment and System Security Plan has been documented, approved, and monitored by management in accordance with the CMS Risk Assessment and System Security Plan Methodologies.	
1. Risks are periodically assessed.	1. Reviewed risk assessment policies.
	2. Reviewed the most recent high-level risk assessment.
	3. Reviewed the objectivity of personnel who performed and reviewed the assessment.
2. A security plan is documented and approved.	1. Reviewed the security plan.
	2. Determined whether the plan covers the topics prescribed by OMB Circular A-130.
3. The plan is kept current.	1. Reviewed the security plan and any related documentation indicating that it has been reviewed and updated and is current.
A.16 Regularly scheduled processes required to support the Medicare contractor's	

continuity of operations (data, facilities or equipment) are performed.	
1. Data and program backup procedures have been implemented.	1. Reviewed written policies and procedures for backing up files.
	2. Compared inventory records with the files maintained off-site and determined the age of these files.
	3. For a selection of critical files, located and examined the backup files. Verified that backup files can be used to recreate current reports.
	4. Determined whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	5. Located and examined documentation.
	6. Examined the backup storage site.
2. Adequate environmental controls have been implemented.	1. Examined the entity's facilities
	2. Interviewed site managers.
	3. Observed that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.
	4. Observed the operation, location, maintenance and access to the air cooling system.
	5. Observed whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.
	6. Determined whether the activation of heat and smoke detectors will notify the fire department.
3. Staff have been trained to respond to emergencies.	1. Interviewed data center staff.
	2. Reviewed training records.
	3. Reviewed training course documentation.
	4. Reviewed emergency response procedures.
	5. Reviewed test policies.
	6. Reviewed test documentation.
	7. Interviewed data center staff.
4. Effective hardware maintenance, problem management, and change management procedures exist.	1. Reviewed hardware maintenance procedures.
	2. Reviewed problem management procedures.
	3. Reviewed change management procedures.
A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components and operations.	

1. Management ensures that corrective actions are effectively implemented.	1. Reviewed the status of prior-year audit recommendations and determined if implemented corrective actions have been tested.
	2. Reviewed recent FMFIA reports.
	3. Reviewed policies and procedures for ensuring that corrective actions are effectively implemented.
	4. Reviewed evidence that management ensures that corrective actions are effectively implemented.
2. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.	1. Reviewed the most recent CMS CSR.
	2. Noted Gaps in compliance as documented in the CMS CSR.
	3. Reviewed management's response to the CSR to ensure that proper controls are in place/are in the process of being in place.
3. Weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. Reviewed policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness.
	2. Inspected evidence that weaknesses are tracked in a formal database (or other manner).
	3. Inspected evidence that planned actions to address all IT security weaknesses are being tracked.
4. Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.	1. Reviewed policies and procedures for preparing CAPs.
	2. Reviewed all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
5. The number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.	1. Reviewed policies and procedures for preparing CAPs.
	2. Reviewed all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed.
	3. Inspected evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
6. Remedial action is being taken for issues noted on audits.	1. Reviewed policies and procedures for taking remedial action for issues noted on audits.
	2. Inspected evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored.
A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.	
1. An incident response capability has been implemented.	1. Interview security manager, response team members, and system users.

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

in accordance with FISMA guidance.	2. Ensured that policies and procedures are in accordance with FISMA standards.

Appendix E: Acronyms and Abbreviations

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

A

AAL	Authorized Access List
AC	Alternating Current
ACA	Annual Compliance Audit
ADM	Administrative
ADP	Automated Data Processing
AFE	Annual Frequency Estimate
AIE	Annual Impact Estimate
AIS	Automated Information System
AISSP	Automated Information Systems Security Program
ALE	Annual Loss Expectancy
ANSI	American National Standards Institute
APF	Authorized Program Facility
ARO	Annualized Rate of Occurrence
ASC	Accredited Standards Committee

B

BI	Background Investigation
BIA	Business Impact Analysis

C

C&A	Certification and Accreditation
CAP	Corrective Action Plan
CAST	Contractor Assessment Security Tool
CCMO	Consortium Contractor Management Officer
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CICG	Critical Infrastructure Coordination Group
CIO	Chief Information Officer
CIS	Center for Internet Security
CISS	CMS Integrated Security Suite
CMP	Configuration Management Plan
CO	Central Office
COMSEC	Communication Security
CMS	Centers for Medicare and Medicaid Services

CPIC	Certification Package for Internal Controls
CPU	Central Processing Unit
CSAT	Computer Security Awareness Training
CSIRC	Computer Security Incident Response Capability
CSR	Core Security Requirement
CWF	Common Working File

D

DASD	Direct Access Storage Devices
DBA	Database Administrators
DBM	Database Management
DC	District of Columbia
DBMS	Database Management System
DES	Data Encryption Standard
DHHS	Department of Health and Human Services
DISA	Defense Investigative Security Agency
DMERC	Durable Medical Equipment Regional Carrier
DOS	Denial of Service
DSL	Digital Subscriber Line
DSS	Digital Signature Standard

E

EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EF	Exposure Factor
E-mail	Electronic Mail
EO	Executive Orders
EVA	External Vulnerability Assessment

F

FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FTI	Federal Tax Information (or Federal tax return information)

G

GAO	General Accounting Office
GSA	General Services Administration
GSS	General Support System

H

HIPAA	Health Insurance Portability and Accountability Act
HISM	Handbook of Information Security Management
HITR	HCFA Information Technology Reference
HSPD	Homeland Security Presidential Directive

I

IA	Information Assurance
IBM	International Business Machines (Corp.)
ID	Identification
IDS	Intrusion Detection System
INFOSEC	Information Systems Security
IP	Internet Protocol
IPL	Initial Program Load
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IRSAP	Internal Revenue Service Acquisition Procedure
ISSO	Information Systems Security Officer
IT	Information Technology
ITMRA	Information Technology Management Reform Act

L

LAN	Local Area Network

M

MA	Major Application
MAC	Medicare Administrative Contractor
MBI	Minimum Background Investigation
MBSA	Microsoft Baseline Security Analyzer
MCM	Medicare Carriers Manual
MCS	Multiple Console Support
MDCN	Medicare Data Communications Network
MIM	Medicare Intermediary Manual
MISPC	Minimum Interoperability Specification for PKI Components
MMA	Medicare Prescription Drug, Improvement, and Modernization Act of 2003
MPS	Minimum Protection Standard
MVS	Multiple Virtual Storage

N

NARA	National Archives and Records Administration
NC	Network Computer

NCSC	National Computer Security Center
NIE	Net Impact Estimate
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NOS	Network Operating System
NSA	National Security Agency
NSC	National Security Council
NSTISSI	National Security Telecommunications and Information Systems Security Committee
NT	New Technology

O

OIG	Office of Inspector General
OIS	Office of Information Services (CMS)
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OTC	On-Time-Cost

P

PC	Personal Computer
PDA	Personal Digital Assistants
PDD	Presidential Decision Directive
PDS	Partitioned Data Sets
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Project (Program) Managers
PO	Project Officer
POA&M	Plan of Action and Milestones
PSGH	CMS Policy Standards and Guidelines Handbook
PSO	Physical Security Officer
PUB	Publication

R

RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFP	Requests for Proposals
RO	Regional Office
ROM	Read Only Memory

S

SA	Security Administrator
SAR	Safeguard Activity Report
SBI	Single Scope Background Investigation (SBI)
SBU	Sensitive but unclassified
SDLC	System Development Life Cycle
SER	Scientific, Engineering, and Research
SHS	Secure Hash Standard
SII	Security/Suitability Investigation Index
SIRT	Security Incident Response Team
SLE	Single Loss Expectancy
SM	System Manager
SMF	System Management Facility
S-MIME	Secure Multi-purpose Internet Mail Extensions
SOW	Statement of Work
SPR	Safeguard Procedures Report
SSA	Social Security Administration
SSC	Systems Security Coordinator
SSG	System Security Group (part of the OIS)
SSL	Secure Socket Layer
SSM	Shared System Maintainers
SSO	Systems Security Officer
SSP	System Security Plan
SSPM	System Security Plans Methodology
SSSA	Senior Systems Security Advisor
STIG	Security Technical Implementation Guide

T

TCP	Transmission Control Protocol
TDES	Triple Data Encryption Algorithm
TLS	Transport Layer Security
TO	Training Office

U

UID	User Identification
UL	Underwriter's Laboratory
U.S.C	United States Code

V

VoIP	Voice over IP

W

WAN	Wide Area Network

Appendix F: - Glossary

(Rev. 6, Issued: 12-09-05, Effective: 09-01-05, Implementation: 01-09-06)

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

Term	Definition
Accountability	The existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established. (FISCAM)
Accreditation	(1) The official management authorization for the operation on an application and is based on the certification process as well as other management considerations. (Automated Information Systems Security Program Handbook [AISSP]) (FIPS PUB 102) (2) A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (NCSC-TG-004)
Action Plan	Part of the CISS functionality, an action plan is a record that indicates the methods by which one or more weaknesses are to be mitigated. An action plan contains milestones and projected completion dates, and is included in the POA&M submission package and any POA&M reports. An action plan is not to be confused with the quarterly CAP submission that Business Partners make to CMS, because the scope of the CAP submission (which contains financial data) exceeds the scope of the CISS.
Application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. (FISCAM)
Application Controls	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. (FISCAM)
Application Programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities. (FISCAM)
Application Programs	See Application.
Application System(s)	A computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system. (AISSP) (FIPS PUB 11-3)

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

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

Term	Definition
Certification (Recertification)	(1) Consists of a technical evaluation of a sensitive application to see how well it meets security requirements. (AISSP) (FIPS PUB 102) (2) A formal process by which an agency official verifies, initially or by periodic reassessment, that a system's security features meet a set of specified requirements.
Checkpoint	The process of saving the current state of a program and its data, including intermediate results to disk or other nonvolatile storage, so that if interrupted the program could be restarted at the point at which the last checkpoint occurred. (FISCAM)
Chief Information Officer (CIO)	The **CIO** is responsible for the implementation and administration of the AIS Security Program within an organization.
Cipher Key Lock	A lock with a key pad-like device that requires the manual entry of a predetermined code for entry. (FISCAM)
Classified Resources/ Data/Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (CNSS)
Code	Instructions written in a computer programming language. (See object code and source code.) (FISCAM)
Cold Site	An information system backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative computing location. (FISCAM)
Command(s)	A job control statement or a message, sent to the computer system, that initiates a processing task. (FISCAM)
Communications Program	A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks. (FISCAM)
Communications Security (COMSEC)	Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (CNSS)
Compact Disc-Read Only Memory (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally read-only. (FISCAM)

Term	Definition
Compatibility	The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are key to achieving compatibility. (FISCAM)
Compensating Control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions. (FISCAM)
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components. (FISCAM)
Compromise	An unauthorized disclosure or loss of sensitive defense data. (FIPS PUB 39)
Computer	See Computer System.
Computer Facility	A site or location with computer hardware where information processing is performed or where data from such sites is stored. (FISCAM)
Computer Network	See Network.
Computer Operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems. (FISCAM)
Computer-related Controls	Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications. (FISCAM)
Computer Resource	See Resource.
Computer Room	Room within a facility that houses computers and/or telecommunication devices. (FISCAM)
Computer Security	See Information Systems Security and Systems Security.
Computer Security Incident Response Capability (CSIRC)	That part of the computer security effort that provides the capability to respond to computer security threats rapidly and effectively. [A CSIRC provides a way for users to report incidents, and it provides personnel and tools for Investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents.] (AISSP – Source: NIST SP 800-3)

Term	Definition
Computer System	(1) A complete computer installation, including peripherals, in which all the components are designed to work with each other. (FISCAM) (2) Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (AISSP) (Computer Security Act of 1987)
Confidentiality	Ensuring that transmitted or stored data is not read by unauthorized persons. (FISCAM)
Configuration Management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. (FISCAM)
Compliance	Refers to the current set of reporting obligations arising from the contractual obligations of business partners to CMS.
Console	Traditionally, a control unit such as a terminal through which a user Communicates with a computer. In the mainframe environment, a **Console** is the operator's station. (FISCAM)
Consortium	Currently consists of four CMS offices (Northeastern, Southern, Midwestern, and Western) that oversee the operations at the Regional Offices.
Consortium Contractor Management Officer (CCMO)	Part of the Regional Consortiums, the **CCMO** is responsible for leading and directing contractor management at the consortium level.
Contingency Plan(s)	(1) Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster. (FISCAM) (2) A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (AISSP) (FIPS PUB 11-3)
Contingency Planning	(1) The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. (ISSPH - Glossary) (2) See contingency plan. (FISCAM)

Term	Definition
Contractors	Non-Federal personnel who perform services for the Federal government under the terms and conditions of a contractual agreement. Contractors need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.
Control Technique	Statements that provide a description of what physical, software, procedural or people related condition must be met or in existence in order to satisfy a core requirement. (Appendix A.)
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text or plain text and other data are transformed into coded form by encryption and translated back to plain text or data by decryption. (FISCAM)
Data	Facts and information that can be communicated and manipulated. (FISCAM)
Data Administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. (FISCAM)
Data Center	See Computer Facility.
Data Communications	(1) The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM) (2) The transfer of data between functional units by means of data transmission according to a protocol. (AISSP) (FIPS PUB 11-3)
Data Control	The function responsible for seeing that all data necessary for processing are present and that all output is complete and distributed properly. This function is generally responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing. (FISCAM)
Data Dictionary	A repository of information about data, such as their meanings, relationships to other data, origin, usage, and format. The dictionary assists company management, database administrators, systems analysts, and application programmers in effectively planning, controlling, and evaluating the collection, storage, and use of data. (FISCAM)

Term	Definition
Data Encryption Standard (DES)	(1) A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data. (FISCAM) (2) The National Institute of Standards and Technology **Data Encryption Standard** was adopted by the U.S. Government as Federal Information Processing Standard (FIPS) Publication 46 [at publication 46-1], which allows only hardware implementations of the data encryption algorithm. (AISSP) (FIPS PUB 11-3)
Data File	See File.
Data Owner	See "Owner." (FISCAM)
Data Processing	The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing. (FISCAM)
Data Security	(1) The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (FIPS PUB 39) (2) See Security Management Function.
Data Validation	Checking transaction data for any errors or omissions that can be detected by examining the data. (FISCAM)
Database	(1) A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer. (FISCAM) (2) A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (AISSP) (FIPS PUB 11-3)
Database Administrator (DBA)	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database. (FISCAM)
Database Management (DBM)	Tasks related to creating, maintaining, organizing, and retrieving information from a database. (FISCAM)

Term	Definition
Database Management System (DBMS)	A software product (DB2, IMS, IDMS) that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions, such as queries or updates from users, and permit centralized control of security and data integrity. (FISCAM)
DBMS	See Database Management System.
Debug (Software)	To detect, locate, and correct logical or syntactical errors in a computer program. (FISCAM)
Degauss	To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (FIPS PUB 39)
Denial of Service (DOS)	Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Synonymous with interdiction. (NCSC-TG-004)
DES	See Data Encryption Standard.
Dial-up(in) Access	A means of connecting to another computer or a network like the Internet, over a telecommunications line using a modem-equipped computer. (FISCAM)
Dial-up Security Software	Software that controls access via remote dial-up. One method of preventing unauthorized users from accessing the system through an unapproved telephone line is through dial-back procedures in which the dial-up security software disconnects a call initiated from outside the network via dial-up lines, looks up the user's telephone number, and uses that number to call the user. (FISCAM)
Disaster Plan	See Contingency Plan.
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (FISCAM)
Disclosure (Illegal Access and Disclosure)	Activities of employees that involve improper systems access and sometime disclosure of information found thereon, but not serious enough to warrant criminal prosecution. These cases should be entered on the Fraud Monitoring and Reporting System.

Term	Definition
Disk Storage	High-density random access magnetic storage devices that store billions of bits of data on round, flat plates that are either metal or plastic. (FISCAM)
Diskette	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case. (FISCAM)
Electronic Data Interchange (EDI)	A standard for the electronic exchange of business documents, such as invoices and purchase orders. Electronic data interchange (EDI) eliminates intermediate steps in processes that rely on the transmission of paper-based instructions and documents by performing them electronically, computer to computer. (FISCAM)
Electronic Mail (e-mail)	The transmission of memos and messages over a network. Within an enterprise, users can send mail to a single recipient or broadcast it to multiple users. With multitasking workstations, mail can be delivered and announced while the user is working in an application. Otherwise, mail is sent to a simulated mailbox in the network server or host computer, which must be interrogated. An e-mail system requires a messaging system, which provides the store and forward capability, and a mail program that provides the user interface with send and receive functions. The Internet revolutionized e-mail by turning countless incompatible islands into one global system. The Internet initially served its own members, of course, but then began to act as a mail gateway between the major online services. It then became "the" messaging system for the planet. (TechEncy)
Electronic Signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. (FISCAM)
Encryption	The transformation of data into a form readable only by using the appropriate key held only by authorized parties. (FISCAM)

Term	Definition
End User(s)	Employees who have access to computer systems and networks that process, store, or transmit information. This is the largest and most heterogeneous group of employees. It consists of everyone, from an executive with a desktop system to application programmers to data entry clerks.
Environmental Controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls. (FISCAM)
Exception Criteria	Exception criteria refers to batch processes that return files or records as not meeting certain predefined criteria for processing.
Execute (Access)	This level of access provides the ability to execute a program. (FISCAM)
Facility(ies)	See Computer Facility.
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record. (FISCAM)
File	A collection of records stored in computerized form. (FISCAM)
Firewall	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. (FISCAM)
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. (FISCAM)
General Controls	The structure, policies, and procedures that apply to an entity's overall computer operations. These include an entity-wide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls. (FISCAM)

Term	Definition
General Support System(s) (GSS)	(1) An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a **general support system** is to provide processing or communication support. (FISCAM) (2) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (OMB Circular A-130)
Guided Media	(1) Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable) (2) Provides a closed path between sender and receiver • Twisted Pair (e.g. Telephone cable) • Coaxial Cable • Optical Fiber (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
Handled	(As in "Data handled.") Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.
Hardware	The physical components of IT, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. (FISCAM)
Hot Site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster. (FISCAM)
Image	An exact copy of what is on the storage medium
Implementation	The process of making a system operational in the organization. (FISCAM)

Term	Definition
Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.
Information	(1) The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people. (FISCAM) (2) Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (AISSP) (OMB Circular A-130)
Information Resource	See Resource.
Information Resource Owner	See Owner.
Information System	The entire collection of infrastructure, organization, personnel, and components used to collect, process, store, transmit, display, disseminate, and dispose of information.
Information Systems Security (INFOSEC)	The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including cryptosecurity, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (AISSP) (NISTIR 4659)
Information Systems Security Officer (ISSO)	(1) Individual responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.
Information Technology (IT)	(1) Processing information by computer. (TechEncy) (2) IT or Information Technology has probably been the most redefined term over the past few years. The definition has varied from simple automation of manual processes using micro-processors to computers to networks to desktop publishing to networking. (Source: U. Texas)
Initial Program Load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program. (FISCAM)
Input	Any information entered into a computer or the process of entering data into the computer. (FISCAM)

Term	Definition
Integrity	With respect to data, their accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users. (FISCAM)
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user. (FISCAM)
Internal Control	A process, effected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. **Internal control** also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring. (Also referred to as Internal Control Structure) (FISCAM)
Internet	When capitalized, the term "**Internet**" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
Investigation(s)	The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system.
IPL	See Initial Program Load.
Job	A set of data that completely defines a unit of work for a computer. A **job** usually includes programs, linkages, files, and instructions to the operating system. (FISCAM)
Junk Mail (e-mail)	Transmitting e-mail to unsolicited recipients. U.S. Federal law 47USC227 prohibits broadcasting junk faxes and e-mail, allowing recipients to sue the sender in Small Claims Court for $500 per copy. (TechEncy)

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

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

Term	Definition
Major Application (MA)	(1) OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application. (FISCAM) (2) An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A major application can be either a major software application or a combination of hardware/software. Its sole purpose is to support a specific mission-related function. (ISSPH - Glossary) (3) An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB Circular A-130) All "Major Applications" require "special management attention." The System Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.
Malicious Software (Code)	The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (AISSP – Source: DHHS Definition, adapted from NIST SP 500-166)
Management Controls	The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used consistent with the organization’s mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision-making. (FISCAM)

Term	Definition
Master Console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands. (FISCAM)
Master File(s)	In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period. (FISCAM)
Material	Refers to data processed, stored, or used in and information generated by an ADP system regardless of form or medium (e.g., programs, reports, data sets or files, records, and data elements).
Media	The physical object such as paper, PC, and workstation diskettes, CD-ROMs, and other forms by which CMS data are stored or transported. The risk to exposure is considered greater when data are in an electronically readable and transmittable form than when the same data are in paper-only form. This is due to the greater volume of information that can be sent in electronic form, the ease and convenience with which the information can be transmitted, and the potential that such information will be intercepted or inadvertently sent to the wrong person or entity.
Methodology	The specific way of performing an operation that implies precise deliverables at the end of each stage. (TechEncy)
Migration	A change from an older hardware platform, operating system, or software version to a newer one. (FISCAM)
Minimum Background Investigation (MBI)	This investigation includes a NACI, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. The MBI is an enhanced version of the NACIC and can be used for selected public trust positions.
Mission Critical	Vital to the operation of an organization. In the past, mission critical information systems were implemented on mainframes and minicomputers. Increasingly, they are being designed for and installed on personal computer networks. (TechEncy)
Misuse of Government Property	The use of computer systems for other than official business that does not involve a criminal violation but is not permissible under CMS policies.

Term	Definition
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received. (FISCAM)
Modification	Loss of integrity of an asset or asset group through the intentional or unintentional alteration of the asset or asset group.
National Agency Check (NAC)	An integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary.
Need-To-Know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. (CNSS)
Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. (FISCAM)
Non-privileged Access	Cannot bypass any security controls.
Object Code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program. (FISCAM)
Office of Information Services (OIS)	CMS Office that ensures the effective management of CMS's information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.
On-line	Available for immediate use. It typically refers to being connected to the Internet or other remote service. When you connect via modem, you are online after you dial in and log on to your Internet provider with your username and password. When you log off, you are offline. With cable modem and DSL service, you are online all the time. A peripheral device (terminal, printer, etc.) that is turned on and connected to the computer is also online. (TechEncy)

Term	Definition
Operating System(s) (OS)	The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running. (FISCAM)
Operational Controls	These controls relate to managing the entity's business and include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards, and (3) does what management directs it to do. (FISCAM)
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy. (FISCAM)
Output Devices	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system. (FISCAM)
Owner	Manager or director with responsibility for a computer resource, such as a data file or application program. (FISCAM)
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs. (FISCAM)
Passwords	(1) A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) (2) Most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications is often easy to circumvent if the user has access to the operating system (and knowledge of what to do).
PDS	See Partitioned Data Set.
Penetration	Unauthorized act of bypassing the security mechanisms of a system. (CNSS)
Penetration Test	An activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.

Term	Definition
Peripheral	A hardware unit that is connected to and controlled by a computer, but external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer. (FISCAM)
Personnel Controls	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause. (FISCAM)
Personal Data	Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
Personnel Security	Refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access. (AISSP – Source: NISTIR 4659) (Also see Personnel Controls)
Physical Access Control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment. (FISCAM)
Physical Security	Refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (SSPS&GH - Glossary) (Source: NISTIR 4659) (Also see Physical Access Control)
Port	An interface between the CPU of the computer and a peripheral device that governs and synchronizes the flow of data between the CPU and the external device. (FISCAM)
Privacy Information	The individual's right to privacy must be protected in Federal Government information activities involving personal information. Such information is to be collected, maintained, and protected so as to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. (OMB Circular A-130)
Privileged Access	Can bypass, modify, or disable the technical or operational system security controls.
Privileges	Set of access rights permitted by the access control system. (FISCAM)

Term	Definition
Probe	Attempt to gather information about an information system or its users.
Processing	The execution of program instructions by the computer's central processing unit. (FISCAM)
Production Control	The function responsible for monitoring the information into, through, and scheduling and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task. (FISCAM)
Production Environment	The system environment where the agency performs its operational information processing activities. (FISCAM)
Production Programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management. (FISCAM)
Profile	A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. (See Standard Profile and User Profile.) (FISCAM)
Program	(1) A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system program, source programs, and object programs are all software programs. (FISCAM) (2) Consists of organized activity that contains ay number of basic elements such as conducting risk assessments; conducting IT security training; establishing an incident response capability; writing, establishing, and enforcing policies and procedures, and processes for planning, implementing, evaluating, and implementing remedial action for addressing weaknesses. (Title III of the E-Government Act)
Program Library	See Library.
Programmer	A person who designs, codes, tests, debugs, and documents computer programs. (FISCAM)
Programming Library Software	A system that allows control and maintenance of programs for tracking purposes. The systems usually provide security, check out controls for programs, and on-line directories for information on the programs. (FISCAM)

Term	Definition
Project Officer (PO)	CMS official (generally located in Central Office business components) responsible for the oversight of other Business Partners. These include Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased. (FISCAM)
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data. (FISCAM)
Public Access Controls	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records. (FISCAM)
Public Domain Software	Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances. (FISCAM)
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (CNSS)
Public Trust Positions	Positions that have the potential for action or inaction by their incumbents to affect the integrity, efficiency, or effectiveness of assigned Government activities. The potential for adverse effects includes action or inaction that could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. (Source: 5 CFR Part 731)
Quality Assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures, and (2) the software meets the functional specifications defined by the user. (FISCAM)

Term	Definition
Read Access	This level of access provides the ability to look at and copy data or a software program. (FISCAM)
Real-time System	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed. (FISCAM)
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item. (FISCAM)
Recovery Procedures	Actions necessary to restore data files of an information system and computational capability after a system failure. (CNSS)
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior. (FISCAM)
Remote Access	The process of communicating with a computer located in another place over a communications link. (FISCAM)
Resource(s)	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and non-computerized records. (FISCAM)
Resource Access Control Facility (RACF)	An access control software package developed by IBM. (FISCAM)
Resource Owner	See Owner. (FISCAM)
Review and Approval	The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network.
Risk	The potential for harm or loss is best expressed as the answers to these four questions: What could happen? (What is the threat?) How bad could it be? (What is the impact or consequence?) How often might it happen? (What is the frequency?) How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" per se. (HISM)

Term	Definition
Risk Analysis	(1) The identification and study of the vulnerability of a system and the possible threats to its security. (AISSP – Source: FIPS PUB 11-3) (2) This term represents the process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures. (HISM)
Risk Assessment	(1) The identification and analysis of possible risks in meeting the agency's objectives that forms a basis for managing the risks identified and implementing deterrents. (FISCAM) (2) This term represents the assignment of value to assets, threat frequency (annualized), consequence (i.e., exposure factors), and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied. The term risk assessment is used to characterize both the process and the result of analyzing and assessing risk. (HISM)
Risk Evaluation	This task includes the evaluation of all collected information regarding threats, vulnerabilities, assets, and asset values in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur. Results are usually expressed in monetary terms on an annualized basis (ALE) or graphically as a probabilistic "risk curve" for a quantitative risk assessment. For a qualitative risk assessment, results are usually expressed through a matrix of qualitative metrics such as ordinal ranking (low, medium, high, or 1, 2, 3). (HISM)

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

Term	Definition
Section 912	Refers to the "Medicare Prescription Drug, Improvement, and Modernization Act of 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors."
Security	(1) The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability. (FISCAM) (2) A technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishments. Also referred to as IT security. (NIST SP 800-16)
Security Administrator (SA)	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks. (FISCAM)
Security Awareness	(1) Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. (NIST SP 800-16) (2) Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences. (NIST SP 800-50)
Security Certification	A formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications. To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system. (NIST Special Publication 800-12)
Security Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

Term	Definition
Security Level Designation	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse) and the operational criticality of data processing capabilities (i.e., the consequences were data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an AIS is assigned for the overall security level designation. (AISSP – Source: DHHS Definition)
Security Management Function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness. (FISCAM)
Security Plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. (FISCAM)
Security Policy	The set of laws, rules, and practices that regulate how an Organization manages, protects, and distributes sensitive information. (NCSC-TG-004)
Security Profile	See Profile.
Security Program	(1) An entity-wide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. (FISCAM) (2) A program established, implemented, and maintained to ensure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its IT systems. (NIST SP 800-16)
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (CNSS)

Term	Definition
Security Requirements Baseline	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security. (CNSS)
Security Software	See Access Control Software.
Security Training	(1) Security training teaches people the [security] skills that will enable them to perform their jobs more effectively. (NIST SP 800-16) (2) Training strives to produce relevant and needed security skills and competencies. (NIST SP 800-50)
Sensitive Application	An application of IT that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (AISSP – Source: OMB Circular A-130)
Sensitive Data	(1) Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (AISSP – Source: OMB Circular A-130) (2) Information whose loss, misuse, unauthorized access to, modification, or destruction, could adversely affect the national interest or the conduct of Federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. (FIPS Pub 102)

Term	Definition
Sensitive Information	(1) Any information whose loss, misuse, unauthorized access, unauthorized disclosure, or improper modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. (from FISCAM) (2) Any information whose loss, misuse, unauthorized access, unauthorized disclosure, or improper modification could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (from the AISSP – Source: Computer Security Act of 1987) (3) CMS Sensitive Information corresponds to "Level-3, High Sensitivity," described in section 4.1.1.3 of this document.
Sensitivity	The degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components. (NIST SP 800-16)
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network. (FISCAM)
Service continuity controls	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (FISCAM)
Significant Change	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (AISSP – Source: DHHS Definition)

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

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

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

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

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

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

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

Term	Definition
Vulnerability	(1) This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. Both expected frequency (ARO) and exposure factor (EF) for fire are increased as a consequence of not having a fire suppression system. (HISM) (2) A flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (NIST SP 800-47)
WAN	See Wide Area Network.
Warning Banner	Verbiage that a user sees or is referred to at the point of access to a system which sets the right expectations for users regarding acceptable use of a computer system and its resources, data, and network access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy.
Wide Area Network (WAN)	(1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) (2) A communications network that connects geographically separated areas. (AISSP – Source: Microsoft Press Computer Dictionary)
Workstation	A microcomputer or terminal connected to a network. **Workstation** can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability. (FISCAM)

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

References:

1. NCSC-TG-004 **–** Rainbow Series, Aqua Book, **Glossary of Computer Security Terms, NCSC-TG-004-88, Library No. S-231, 238**. Issued by the National Computer Security Center (NCSC).
2. FISCAM – Federal Information System Controls Audit Manual, GAO/AIMD-12.19.6
3. AISSP – Automated Information Systems Security Program Handbook, DHHS, http://wwwoirm.nih.gov/policy/aissp.html, (for Source references see document)
4. Micki Krause and Harold F. Tipton, Handbook of Information Security Management (HISM), Imprint: Auerbach Publications, Publisher: CRC Press LLC, ISBN: 0849399475.
5. DoN - Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A, Aug. 3, 1982. (Glossary)
6. CNSS – Committee on National Security Systems (CNSS) National Information Assurance Glossary, CNSS Instruction No. 4009, Revised May 2003
7. TechEncy – Technical Encyclopedia of definitions supported by TechWeb.com

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