

Business Partners Systems Security Manual



CENTERS FOR MEDICARE AND MEDICAID SERVICES (CMS)
SECURITY AND STANDARDS
7500 SECURITY BOULEVARD
BALTIMORE, MD 21244-1850

March 05, 2004

CMS/Business Partners Systems Security Manual

1. Introduction
2. IT Systems Security Roles and Responsibilities
 - 2.1 Consortium Contractor Management Officer and CMS Project Officer (CCMO/PO)
 - 2.2 The (Principal) Systems Security Officer (SSO)
 - 2.3 System Owners/Managers
 - 2.4 System Maintainers/Developers
 - 2.5 Personnel Security/Suitability
3. IT Systems Security Program Management
 - 3.1 System Security Plan (SSP)
 - 3.2 Risk Assessment
 - 3.3 Certification
 - 3.4 Information Technology Systems Contingency Plan
 - 3.5 Compliance
 - 3.5.1 Annual Compliance Audit
 - 3.5.2 Corrective Action Plan
 - 3.6 Incident Reporting and Response
 - 3.6.1 Computer Security Incident Response
 - 3.7 System Security Profile
 - 3.8 Fraud Control
4. IT Systems Sensitivity/Criticality Determinations
 - 4.1 Information Security Levels
 - 4.1.1 Sensitivity Levels for Data
 - 4.1.1.1 Level 1: Low Sensitivity
 - 4.1.1.2 Level 2: Moderate Sensitivity
 - 4.1.1.3 Level 3: High Sensitivity
 - 4.1.1.4 Level 4: High Sensitivity and National Security Interest
 - 4.1.2 Criticality Levels for IT Systems

- [4.1.2.1 Level 1: Low Criticality](#)
- [4.1.2.2 Level 2: Moderate Criticality](#)
- [4.1.2.3 Level 3: High Criticality](#)
- [4.1.2.4 Level 4: High Criticality and National Security Interest](#)
- [4.2 Sensitive Information Protection Requirements](#)
- [4.2.1 Restricted Area](#)
- [4.2.2 Security Room](#)
- [4.2.3 Secured Interior/Secured Perimeter](#)
- [4.2.4 Container](#)
- [4.2.4.1 Locked Container](#)
- [4.2.4.2 Security Container](#)
- [4.2.4.3 Safes/Vaults](#)
- [4.2.5 Locking Systems for Secured Areas and Security Rooms](#)
- [4.2.6 Intrusion Detection Equipment \(IDS\)](#)

5. Internet Security

Appendices

[Attachment A \(CSRs\)](#)

Appendices

[Appendix A- CMS Core Security Requirements and the Contractor Assessment Security Tool \(CAST\)](#)

[Appendix B- Medicare Information Technology \(IT\) Systems Contingency Planning](#)

[Appendix C- An Approach to Fraud Control](#)

[Appendix D- Acronyms and Abbreviations](#)

[Appendix E- Glossary](#)

1.0 Introduction

(Rev. 4, 03-05-04)

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

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

This manual addresses the following key business partner security elements:

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

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

- Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to provider of service.
- Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits.
- Public Law 93-579, The Privacy Act of 1974, as amended.
- Public Law 99-474, Computer Fraud & Abuse Act of 1986.
- Public Law 100-235, Computer Security Act of 1987.
- Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35.
- Public Law 104-106, Clinger-Cohen Act of 1996 (formerly called Information Technology Management Reform Act).
- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA), 1996.
<http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm>
- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996.

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

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

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

- Code of Federal Regulations, Regulation 5 CFR Part 731 – Suitability, 5CFR731
<http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html>
- FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25 U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, PUB 46-3.
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
- CMS Internet Security Policy
www.cms.hhs.gov/it/security
- *CMS Information Security Risk Assessment (RA) Methodology, Version # 1.1 September 12, 2002.*
<http://www.cms.hhs.gov/it/security/>

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

2.0 IT Systems Security Roles and Responsibilities (Rev. 3, 03-28-03)

2.1 Consortium Contractor Management Officer and CMS Project Officer (CCMO/PO) (Rev. 3, 03-28-03)

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 Project Officers (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 systems security plans and reports including security incident reports.

Provide the personnel and technical assistance necessary to respond to CMS security policies and procedures.

2.2 The (Principal) Systems Security Officer (SSO)

(Rev. 4, 03-05-04)

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

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

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

- Facilitating the Medicare IT system security program and assuring necessary safeguards are in place and working.
- Coordinating system security activities throughout the organization.
- Ensuring that IT systems security requirements are considered during budget development and execution.
- Reviewing compliance of all components with the CMS Core Security Requirements and reporting vulnerabilities to management.
- Establishing an incident response capability, investigating systems security breaches, and reporting significant problems (see Section 3.6) to business partner management, and CMS.
- Ensuring that technical and operational security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes.
- Ensuring that IT systems security requirements are included in RFPs and subcontracts involving the handling, processing, and analyzing of Medicare data.
- Maintaining systems security documentation in the Systems Security Profile for review by CMS and external auditors.
- Cooperating in all official external evaluations of the business partner's systems security program.
- Facilitating the completion of the Risk Assessment (see Section 3.2).

- Ensuring that an operational Information Technology Systems Contingency Plan is in place and tested (see Section 3.4).
- Documenting and updating the Corrective Action Plans (see Section 3.5). Updates follow issuance of new requirements, risk assessment, internal audit, external evaluation, and, of course, the target dates themselves. (The schedule and updates are highly sensitive and should have limited distribution.)
- Keeping all elements of the business partner's System Security Profile secure (see Section 3.7).
- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix B).

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

2.3 System Owners/Managers (Rev. 3, 03-28-03)

Business partner System Owners/Managers have the responsibility to:

Determine and document the data sensitivity and application criticality of the resources for which they are responsible.

Identify appropriate security level designation 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. 3, 03-28-03)

CMS is currently reviewing business partner position security and personnel investigative requirements. The results of this review will be published when completed. In the interim, CMS is publishing the following minimum investigative requirement for all prospective business partner and contractor employees requiring access to CMS sensitive information. A contractor also can be a subcontractor to a CMS business partner.

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 is not merely based on position or title and favorable results from a background check. This background check for prospective and existing employees (if not previously completed) should, at a minimum, include: contacting references provided by the employee, and contacting the local law enforcement agency or agencies.

3.0 IT Systems Security Program Management

(Rev. 4, 03-05-04)

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

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

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

Table 3.1. Planning Table

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

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.1 System Security Plans	Each Federal fiscal year for each GSS and MA, or upon significant change.	Systems Security Profile. SSO CMS CO	System Security Plans are to be reviewed and updated as necessary and are to be discussed within the Certification Package. More information about System Security Planning can be found in the CMS SSP Methodology.	<input type="checkbox"/>
3.2 Risk Assessment (Report)	Every year or upon significant change.	Systems Security Profile CMS CO	<i>Risk Assessments are to be discussed within the Certification Package. The Risk Assessment Report is an attachment of the System Security Plan.</i> More information about Risk Assessment Reports can be found in the CMS Information Security RA Methodology.	<input type="checkbox"/>
3.3 Certification	Each Federal fiscal year.	CCMO/PO with a copy to CMS CO.	<i>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.</i>	<input type="checkbox"/>

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

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
<p>3.5 Compliance</p>	<p>Each Federal Fiscal year.</p>	<p><i>CCMO/PO</i></p> <p><i>Systems Security Profile</i></p> <p><i>SSO</i></p> <p><i>CMS CO</i></p> <p><i>May be stored as paper documents, electronic documents, or a combination.</i></p>	<p>There are two (2) components to compliance:</p> <p>(1) Annual Compliance Audit:</p> <p>Once a year, an independent audit will be performed on four (4) categories of the CMS Core Security Requirements to validate the self-assessment. CMS will determine the four categories the audit will validate by way of a Program Memorandum (PM).</p> <p>(2) Corrective Action Plan</p> <p>Corrective Action Plans address findings of annual systems security assessments including the Annual Compliance Audit, annual core security requirements review, SAS 70 audits (if any), and <i>CFO</i> controls audits (if any).</p> <p>CAST (see Appendix A, Section 2) will record all items assessed as “Partial” or “Planned.” The Corrective Action Plan addresses all “Partial” and “Planned” items, along with their “Comments/Explanations” and “Projected Completion Dates.”</p>	<p><input type="checkbox"/></p> <p><input type="checkbox"/></p>
<p>3.6 Incident Reporting and Response</p>	<p>As necessary.</p>	<p>CCMO/PO</p> <p>Systems Security Profile</p>	<p>The HIPAA also addresses Incident Reporting information.</p>	<p><input type="checkbox"/></p>

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.7 System Security Profile	As necessary.	On file in the Security Organization.		<input type="checkbox"/>

LEGEND:

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

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

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

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

- Northeast Consortium
Consortium Contractor Management Officer
Philadelphia Regional Office, Suite 216
The Public Ledger Building
150 S. Independence Mall West
Philadelphia, PA 19106
215-861-4191
- Southern Consortium
Consortium Contractor Management Officer
Atlanta Regional Office
Atlanta Federal Center, 4th Floor
61 Forsyth Street, SW, Suite 4T20
Atlanta, GA 30303-8909
404-562-7250

- Midwest Consortium
Consortium Contractor Management Officer
Chicago Regional Office
233 N. Michigan Avenue, Suite 600
Chicago IL 60601
312-353-9840
- Western Consortium
Consortium Contractor Management Officer
San Francisco Regional Office
75 Hawthorne St. 4th and 5th Floors
San Francisco, CA 94105-3901
415-744-3628

3.1 System Security Plan (SSP)

(Rev. 4, 03-05-04)

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

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

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

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

addition, the SSP forms the primary reference documentation for testing and evaluation, whether by CMS, the GAO, or other oversight bodies. The SSP is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, these security plans should be distributed only on a need-to-know basis.

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

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

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

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

A newly developed or updated SSP including the ORIGINAL signed and dated CMS SSP certification form (Tab A, Appendix A of the CMS SSP Template) must be sent to the CMS Central Office (Security and Standards Group; Mail Stop N2-14-26; 7500 Security Blvd.; Baltimore, MD 21244-1850). These documents must be received by CMS ten (10) working days after they have been developed, updated, or recertified. These documents must be

submitted in hard copy and on CD-ROM. Please be advised that this information should not be submitted to the CMS Central Office via email. Registered mail or its equivalent should be used.

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

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

3.2 Risk Assessment

(Rev. 4, 03-05-04)

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

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

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

All RAs must be recertified within 365 days from the last date certified. Medicare Contractors must review their RA(s) prior to recertification to determine if an update is needed. An RA must be performed if a significant change³ 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 posture. Documentation of the review and/or the updated RA must be placed in the Medicare Contractor's System Security Profile. The updated RA(s) must also be mailed to the CMS Central Office. The RA used to support a SSP(s) cannot be dated more than 12 months earlier than the SSP certification date.

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

³ The National Institute of Standards and Technology defines "significant change to an information systems is any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."

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

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

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

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

3.3 Certification

(Rev. 4, 03-05-04)

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

Each contractor is required to self-certify to CMS its IT systems security compliance within each Federal fiscal year. This security certification will be included in the *Certification Package for Internal Controls (CPIC)*. CMS will continue to require annual, formal re-certification within each fiscal year no later than September 30, including validation at all levels of security as described in this manual.

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

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

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

3.4 Information Technology Systems Contingency Plan

(Rev. 4, 03-05-04)

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

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

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

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

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

3.5 Compliance (Rev. 3, 03-28-03)

3.5.1 Annual Compliance Audit

(Rev. 4, 03-05-04)

Each business partner must conduct an Annual Compliance Audit on four (4) out of the ten (10) categories of the CMS Core Security Requirements. A compliance audit is a performance review of a business partner's systems security program that tests whether the systems security controls

comply with CMS' CSRs (Appendix A of this manual) and are implemented properly. The audit will be documented through an Annual Compliance Audit Report.

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

Government auditing standards dictate business partner staff assigned to conduct an audit should possess adequate professional proficiency for the tasks required⁴. An audit team should include audit skills and familiarity with implementation of the physical and IT security features utilized by the business partner or required by CMS. Required audit skills include proficiency in basic auditing tasks, communicating, and project management. An internal audit department with these qualifications may perform the Annual Compliance Audit.

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

The Annual Compliance Audit Report must include the following:

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

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

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

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

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

make a formal recommendation to the CCMO/Consortium Contractor Management Staff (CCMS) to verify that the CAP has been satisfied.

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

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

3.5.2 Corrective Action Plan

(Rev. 4, 03-05-04)

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

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

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

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

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

Business partners are strongly encouraged to develop a project plan for all CAPs that cannot be resolved within 30 calendar days. A project plan enables the owner and other interested parties

(i.e. CMS and auditors) to track its progress and ensure they are on schedule as planned. Project plans provide more detail than the general information contained in a CAP. The project plan should document the safeguard, (major) milestone dates, and the necessary steps or actions taken to resolve the CAP. These steps may include activities, responsible entities, and cost (if any). Supporting documentation, such as invoices, should be included as attachments to the project plan. The project plan should be maintained in the systems security profile and made available for review.

3.6 Incident Reporting and Response (Rev. 3, 03-28-03)

An incident is the act of violating the security policy, procedure, or a core security requirement. The business partner will use their Security policy and procedures in determining that a reportable security incident occurred. 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 are:

A penetration or denial of service attack with impact on operations;

An information disclosure with risk to privacy information or public relations impact; and

Instances of computer virus not handled by anti-virus software.

3.6.1 Computer Security Incident Response

(Rev. 4, 03-05-04)

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

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

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

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

3.7 System Security Profile (Rev. 3, 03-28-03)

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

Risk Assessment;

Completed CAST Self Assessment(s);

Annual Compliance Audit Report;

Information Technology Systems Contingency Plans;

Security reviews undertaken by DHHS OIG, CMS, IRS, GAO, consultants, subcontractors, and business partner security staff;

Corrective Action Plan for each security review;

System Security Plan (for each GSS and MA); and

Systems security policies and procedures.

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. 3, 03-28-03)

Business partners are required to safeguard systems against fraud. The CMS Core Security Requirements 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, CMS Core Security Requirements and the Contractor Assessment Security Tool (CAST) and Appendix C, An Approach to Fraud Control.

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. 4, 03-05-04)

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

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

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

Table 4.1. Summary of Sensitivity and Criticality Levels

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

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

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

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

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

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

4.1.1 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. 3, 03-28-03)

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 Core Security Requirements. The data in this category requires the greatest number and most stringent 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 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 (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. These data are 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)

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. 3, 03-28-03)

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 are considered to have moderate sensitivity (Level 2).

4.1.2.3 Level 3: High Criticality (Rev. 3, 03-28-03)

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 are 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. 4, 03-05-04)

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

4.2 Sensitive Information *Protection* Requirements

(Rev. 4, 03-05-04)

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

Table 4.2. Protection Alternative Chart

	<i>Perimeter Type</i>	<i>Interior Area Type</i>	<i>Container Type</i>
<i>Alternative #1</i>	<i>Secured</i>		<i>Locked</i>
<i>Alternative #2</i>	<i>Locked</i>	<i>Secured</i>	
<i>Alternative #3</i>	<i>Locked</i>		<i>Security</i>

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

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

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

4.2.1 Restricted Area

(Rev. 4, 03-05-04)

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

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

4.2.2 Security Room

(Rev. 4, 03-05-04)

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

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

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

4.2.3 Secured Interior/Secured Perimeter

(Rev. 4, 03-05-04)

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

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, **or** any lesser-type partition (i.e., slab-to-slab walls) supplemented by UL-approved electronic IDS and fire detection systems.*
- Unless electronic IDS devices are used, all doors entering the space must be locked, and strict key or combination control should be exercised.*
- In the case of a fence and gate, the fence must have IDS devices **or** be continually guarded, and the gate must be either guarded or locked with intrusion alarms.*
- The space must be cleaned during working hours in the presence of a regularly assigned employee.*

4.2.4 Container

(Rev. 4, 03-05-04)

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

4.2.4.1 Locked Container

(Rev. 4, 03-05-04)

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

4.2.4.2 Security Container

(Rev. 4, 03-05-04)

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

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

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

4.2.4.3 Safes/Vaults

(Rev. 4, 03-05-04)

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

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

4.2.5 Locking Systems for Secured Areas and Security Rooms

(Rev. 4, 03-05-04)

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

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

4.2.6 Intrusion Detection Equipment (IDS)

(Rev. 4, 03-05-04)

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

5.0 Internet Security

(Rev. 4, 03-05-04)

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

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

(Rev. 4, 03-05-04)

1.0 *CMS Core Security Requirements*

2.0 *The Contractor Assessment Security Tool (CAST)*

2.1.1 All Responses:

2.1.2 Yes Responses:

2.1.3 No Responses:

2.1.4 Partial Responses:

2.1.5 Planned Responses: (Rev)

2.1.6 N/A Responses:

1.0 *CMS Core Security Requirements*

(Rev. 4, 03-05-04)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

www.cms.hhs.gov/it/security

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

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

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

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

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

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

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

Category	Description
	capability to process, handle, and protect the information it is entrusted with.
Application Software Development and Change Control	These controls address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information.
Application System Authorization Controls	These controls address the processing of Medicare data in a manner that ensures that only authorized transactions are entered into the information processing system.
Application System Completeness Controls	These controls ensure that all system transactions are processed and that any missing or duplicate transactions are identified and a remedy implemented.
Application System Accuracy Controls	These controls address the accuracy of all data entered into systems for processing, handing, and storage. Data must be valid and accurate. All invalid, erroneous, or inaccurate data must be identified and corrected.
Networks	These controls address the network structure. The network structure must be protected and the data transmitted on the networks must be protected.

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

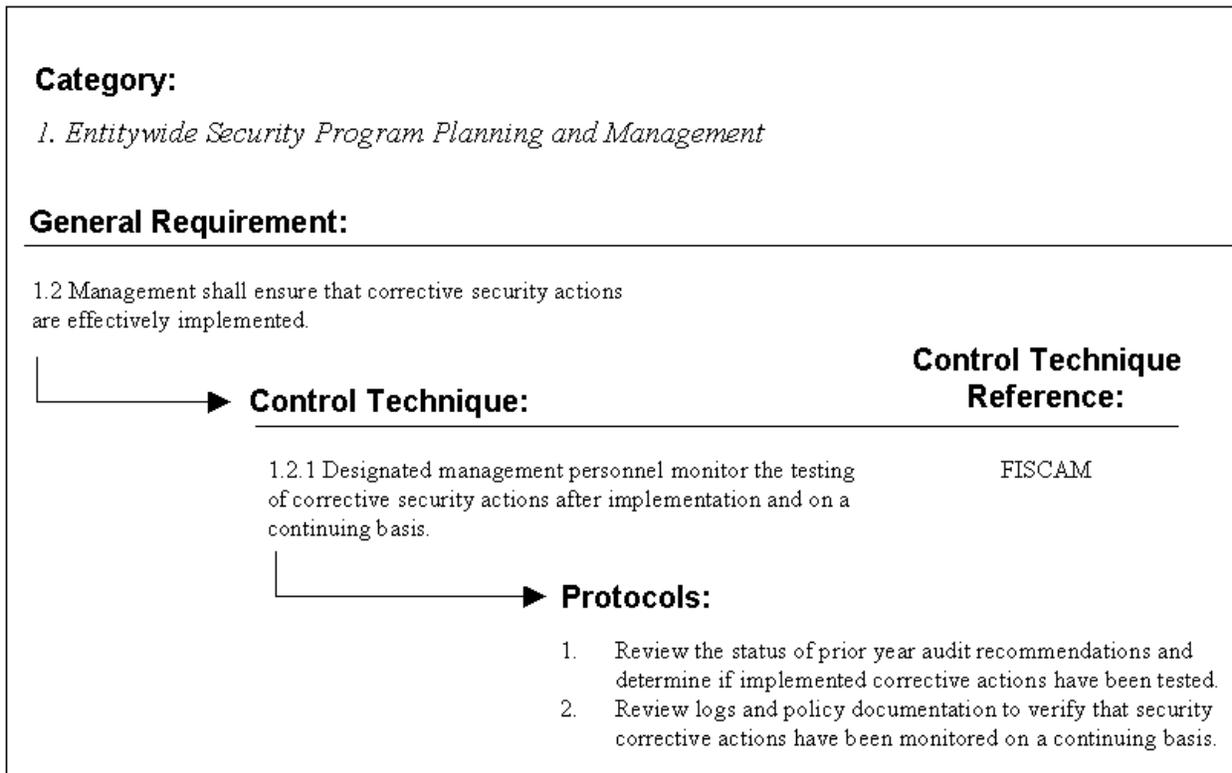


Figure A-1. Relationship Among General Requirements, Control Techniques, and Protocols

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

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

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

- **Guidance** - Additional guidance has been developed to clarify issues and provide additional information regarding each CSR. This information is available in the CAST during the self-assessment process, and may be printed from the forms menu.
- **Related CSRs** - Each CSR may be related to one or more other CSRs. It may be important that CSR responses be coordinated between these related CSRs. Business partners should take care to ensure that these related CSR responses are not conflicting. This information is available in the CAST during the self-assessment process, and may be printed from the forms menu.
- **CSR Responsibility** - A matrix has been developed jointly with CMS and business partner security experts to indicate where responsibility may lie for addressing the requirement of each CSR. This matrix indicates a best estimate of whether a particular CSR is applicable to a given contract type. While this matrix is not meant to be used as a requirements document, it does give business partners and CMS reviewers an indication of whether a particular CSR should be addressed by a given business partner. This information is available in the CAST during the self-assessment process, and may be included in output printed from the “Print Reports.”

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

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

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

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

2.0 The Contractor Assessment Security Tool (CAST)

(Rev. 4, 03-05-04)

Core Security Requirement Responses

(Rev. 4, 03-05-04)

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

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

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

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

2.1.1 All Responses

(Rev. 4, 03-05-04)

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

- a) When entering information into CAST, the business partner will provide specific information in the CAST Explanation/Comment field as to the status of compliance with the applicable requirement. CAST can then produce a pre-formatted report of self-assessment results and graphical analysis.*
- b) Each CSR requires a “Status” to be selected, and each CSR requires a detailed explanation in the CAST Explanation/Comment field to describe and explain the compliance status. In addition, all CSR responses must include a complete description of Who, What, Where, Why, and How each CSR is or is not in compliance, depending on the CSR status selection.*
- c) Where a merging of responsibilities occurs between business partners (such as the interface between Data Centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities should be provided in the Explanation/ Comments field. The description should include local responsibilities as well as those that are perceived to be responsibilities of some other CMS business partner.*
- d) Each CSR in the CAST includes a Gap Responsibilities matrix that identifies the likely responsibility of each CSR by CMS contract type (i.e., Part A, Part B, DMERC, etc.). The purpose of the applicability matrix is not to summarily include or exclude CSRs from a particular contract type. The applicability matrix is designed only as a guide to business partners. CMS recognizes that system configurations vary widely throughout the business partner community. Therefore, each business partner must evaluate each CSR as to applicability to its own systems.*
- e) Business partners should be aware that even if data processing duties are subcontracted out to either another CMS business partner (such as a Data Center) or to some third-party subcontractor (such as a business services company), responsibility for the implementation of security controls ultimately resides with the primary contract holder. Business partners should coordinate the establishment of boundaries for specific issues. While this does not necessarily require a sharing of self-assessment responses, it does require that business partners communicate and coordinate among themselves such that interfaces of responsibilities for particular CSRs are addressed by all responsible entities without gaps in coverage.*
- f) Business partners should also be aware of the CSR terms included in the BPSSM Glossary (Appendix E) and address the CSRs as they apply within their local environment. For example, the term “data center” refers to any site or location where information is processed (e.g., claims entry and processing) and is not limited to a CMS Data Center (e.g., mainframe). A “system” may include mainframe systems, desktop systems, workstations and servers, networks, and any platform regardless of the operating system. “System software” includes the operating system and utility programs (e.g., workstation, server, and network software and utilities) and is distinguished from*

application software. “Application software” includes the standard system (i.e., Major Application) but it also includes any computer program that manipulates data or performs a specific function (e.g., front-end and back-end applications).

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

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

2.1.2 Yes Responses

(Rev. 4, 03-05-04)

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

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

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

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

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

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

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

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

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

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

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

- e) **Safeguards** – The “Safeguard” button is disabled for a response with a status of “Yes.”

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

Example entry for a CSR with a response status of “Yes”:

“Security Awareness Training is conducted during initial employee orientation and every year during the month of November for all employees and contractors. It includes all aspects outlined in the CSR Control Techniques as documented in company policy NG 7541-S3. The

records of attendance are maintained in the Corporate Training Office, on the fifth floor of Bldg. #5 (cabinet #5). POC is Jim Socrates (401) 555-1212.”

2.1.3 No Responses

(Rev. 4, 03-05-04)

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

- a) **Who** is the principal POC for questions involving this requirement?
 - i) *The principal POC should be clearly delineated. This will ensure that detailed questions and requests for clarification can be addressed quickly and efficiently. While CMS will work directly with the SSO for resolution of issues, recording of the individual POC for each CSR will greatly simplify the SSO’s resolution process.*
- b) **Why** is this CSR not being fully met? What efforts are underway or have been completed in an attempt to fully resolve this issue?
 - i) **Funded vs. Unfunded plans:**
 - (1) *A funded plan consists of a documented timetable and existing funding. Funding may consist of corporate funding, existing Line One funding, and/or some other previously awarded funding.*
 - (a) *If a funded plan exists for implementation of a suitable control, but has not yet been implemented, then a detailed explanation must be provided outlining the obstacles to implementation of any funded Safeguards.*
 - (2) *A plan is considered unfunded if it requires additional funding that is not currently allocated or available for Safeguard implementation. A Safeguard should be generated with appropriate funding requirements indicated.*
 - (a) *If there is currently no funded plan for meeting compliance with this CSR, a detailed explanation must be provided outlining all of the obstacles to implementation of a suitable control (including Safeguards and funding requirements).*
- c) **How** did you verify this status with CMS?
 - i) *CMS expects all CSRs to be addressed by all business partners. If the business partner does not meet the requirements of any CSR and has no plans to implement the*

- CSR control techniques, written notification must be provide to CMS and acknowledged by CMS. This written notification should include a detailed explanation of why the CSR control techniques are not being met and why the business partner does not intend to implement them.*
- ii) Include the following information with CMS-approved “No” responses:*
- (1) Date CMS acknowledged the response,*
 - (2) CMS office that acknowledged the response, and*
 - (3) Method of CMS acknowledgement (e.g., e-mail, letter, phone call).*
- iii) Describe any circumstances that may have prevented implementation of a suitable control to date. While this explanation will not alleviate responsibility for the CSR, it will reduce inquiries by CMS during the evaluation phase of business partner self-assessments.*
- d) Safeguards – The “Safeguard” button is enabled for a response with a status of “No.” Safeguards should be developed to address the CSR. If funding is required to change systems, policies, or procedures in order to become compliant with this CSR, the Safeguards should describe (in detail) the funding requirements. Not all Safeguards require additional funding. Many Safeguards are already funded through existing funding sources and should therefore be answered with a status of “Planned.” Details on how to develop Safeguards within the CAST are provided in a later section.*

Example entry for a CSR with a response status of “No”:

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

2.1.4 Partial Responses

(Rev. 4, 03-05-04)

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

explanation of the Who, What, Where, Why, and How. These minimum requirements are listed below:

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

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

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

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

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

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

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

i) **Funded vs. Unfunded plans:**

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

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

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

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

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

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

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

- ii) *Describe in detail how the remaining Control Techniques will be brought into compliance by the Projected Completion Date.*
- iii) *In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.*

f) *Enter a “Projected Completion Date”:*

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

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

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

*“We use a mainframe and an off-site data storage facility connected via a T1 line and triple-DES encryption. However, the local corporate distributed network (WAN), which may process some administrative documents containing sensitive patient information, is connected via DSL and T1 lines to remote facilities without encryption. Additional network encryption devices are required for the local corporate distributed LAN. Documentation on our existing and planned encryption techniques is maintained in the Security Department, on the second floor of Bldg. #2 (cabinet #2). The POC in the Security Department is Iam Secure (401) 555-1234.
Projected Completion Date: 2/10/2002”*

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

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

2.1.5 Planned Responses

(Rev. 4, 03-05-04)

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

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

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

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

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

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

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

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

i) **Funded plans:**

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

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

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

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

i) Explain in detail how all components of the planned controls will be implemented by the Projected Completion Date. When a CSR includes multiple elements or

requirements, planned controls must be explained in detail for each element or requirement in the CSR.

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

f) Enter a “Projected Completion Date”:

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

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

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

Example entry for a CSR with a response status of “Planned”:

“A training plan and training materials do not exist for new employee orientation training. New employee training is being developed in a joint effort between the Security Department and the IT Training Department. The security training outline is complete and on file in the Corporate Training Office on the fifth floor of Bldg. #5 (cabinet #5). No additional Safeguards or funding is required to meet the requirements of this CSR. The training POC is Jim Socrates (401) 555-1212. The POC in the Security Department is Iam Secure (401) 555-1234

Projected Completion Date: 2/10/2002”

2.1.6 N/A Responses

(Rev. 4, 03-05-04)

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

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

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

b) Why is this CSR not applicable?

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

c) How did you verify this status with CMS?

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

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

- (1) Date CMS approved the response,*
- (2) CMS office that approved the response, and*
- (3) Method of CMS approval (e.g., e-mail, letter, phone call).*

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

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

Safeguards

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

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

The screenshot shows a software window titled "Safeguard". The interface includes a "Title:" text box at the top. Below it is a large "Description:" text area. To the left of the description area is a "Priority:" dropdown menu with a "Change Priority" button below it. At the bottom of the window, there are several sections: "Total Safeguard Cost:" with a text box, "% Cost Applied to CMS:" with a text box containing "100.00%", a "Spell Check" button, "Responsibility:" with radio buttons for "Generic" (selected) and "Shared System Maintainer", "Safeguard Type" with a dropdown menu, and "Projected Recurring CMS Cost:" with a text box and a "Close" button. A red rectangular box obscures the "Safeguard cost to CMS for this contract:" field.

Figure A-3. Safeguard Cost Form

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

Recommendations for generating Safeguards:

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

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

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

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

Examples:

“SG001 - Purchase and implement virus protection software”

“SW002 - Purchase and install Network Encryption Software”

“HW003 - Install Firewall host for MVS system”

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

Example:

The firewall Safeguard will include:

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

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

- 3) **Priority:** This is the priority of this Safeguard as perceived by the user (business partner). The priority reflects the business importance to the business partner. Priorities should be incremental starting at 1 and ascending to the total number of Safeguards (i.e., 1 through 17 for a total of 17 Safeguards). One (1) is the highest priority.
- 4) **Total Safeguard cost:** This section will include the Total cost of the Safeguard for the first year of implementation. These will include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. Note: This submission will be used for budgetary purposes it must be as accurate as feasible. It is advised that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted.
- 5) **Projected Recurring Cost:** This is the projected recurring cost to CMS to maintain this Safeguard for the following FY. This includes depreciation, amortization, etc. Cost associated with continuing funding should be added to subsequent line one charges where applicable.

- 6) **% Cost Applied to CMS:** This is the percentage of cost of the Safeguard that will be charged to CMS. This is the percentage of cost that CMS will carry for Safeguards that will be shared between CMS (Medicare) systems and corporate systems.
- 7) **Safeguard Type:** This is the type of Safeguard that is planned. The user will choose from a drop-down list of Safeguard type that includes Outsource, Hardware, Software, Facilities, and/or Personnel. The Safeguard can be of any combination of one or more of the five possibilities.
- 8) **Responsibility:** This is a radio button that assigns responsibility to either the entity performing the self-assessment, or to the System Maintainer (for Shared Systems Software changes required to meet this CSR). Safeguards assigned to the standard system maintainer shall not be funded through the entity completing this self-assessment. However, these Safeguards will be reviewed and forwarded to the Shared System Maintainer, where applicable.
- 9) **Safeguard cost to CMS for this contract:** This is the system calculated (by CAST) cost to CMS for implementing this Safeguard. It is calculated using the following formula:
$$(\text{Total Safeguard cost}) \times (\% \text{ Cost Applied to CMS}) \times (\% \text{ CMS Cost Applied to this contract}) = \text{Total current FY CMS cost for this contract.}$$

Appendix B

Medicare Information Technology (IT)

Systems Contingency Planning

3.0 Definition of an Acceptable Contingency Plan

(Rev. 4, 03-05-04)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3 Test Types

Contingency plan test guidance suggests three types of testing:

- Walkthrough
- Simulation/modeling
- Live.

These are defined below:

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

Simulation involves taking some physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team do the same a the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

- **Live:** *This is the most complete and expensive test to accomplish. It involves doing physically what would actually be accomplished if an emergency occurred. People and materials would be moved to an alternate site for the test. Servers would actually be shut down to reduce capability. Power would actually be shut off. Live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications and people at the alternate site would be set into action and begin functioning as the primary site to support operations.*

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

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

- Not testing end-to-end means *that* some links, processes, or subsystems are missed.
 - What is the risk in not doing end-to-end?
- Live end-to-end testing can be very expensive!

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

6.3.1 Live vs. Walkthrough

(Rev. 4, 03-05-04)

- High-level testing can *take the form of* a walkthrough test.
- *A walkthrough* 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 *and* time. If that cost outweighs the “cost” of the risk of not doing live testing, then “live” testing should probably be ruled out.

6.3.2 End-to-End

(Rev. 4, 03-05-04)

This kind of testing 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 data base through to the response;
 - MSP check request through to check issue and back to MSP.
- Evaluate complexity and cost.
 - The decision on how to test critical functions, processes, and systems must carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost out weighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.
- *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.

7.0 Minimum Recovery Times

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).

8.1 Business Partner Management

(Rev. 4, 03-05-04)

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

- Test Results
- Corrective Action Plans,
- Retest Plans,
- Memos of Understanding/Formal Arrangement Documents
- Changes *to* storage and backup/alternate site facilities.

11.0 Checklist

(Rev. 4, 03-05-04)

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

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

1. Introduction

Does the contingency plan contain:

- Background
 - Is a history of the plan provided? Are the physical environment and the systems discussed?
- Purpose/Objective
 - What does the plan address? Why was it written? What is hoped to be accomplished by using the plan?
- Management Commitment Statement
 - Has the contingency plan been approved by management and the SSO? Once the contingency plan is created, reviewed and ready for distribution, it should be approved by site, operations and IS management, and the SSO.
- Scope
 - Are the boundaries of the plan indicated? What organizations are involved, not involved?
 - Organizations
 - Systems
 - Boundaries?
- IT Capabilities and Resources
 - Is the focus of the plan on IT systems, capabilities, and resources?
- Contingency Plan Policy
 - Priorities
 - Continuous operation

- Are there functions, processes, or systems that are required to continue without interruption?
 - Recovery after short interruption
 - Which functions, processes, or systems can be interrupted for a short time?
 - Minimum Recovery Times
 - Are recovery times stated?
 - Standalone Units
 - Does a contingency plan exist for any standalone workstation? A key part of a contingency plan should address any standalone workstations that are part of the critical operations environment. It should state where backup software and support data for these workstations is stored.
- Is the plan reviewed and approved by other key affected persons?

2. Assumptions

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

3. Authority/References

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

4. Definition of what the Contingency Plan Addresses

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

5. *Three phases defined*

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

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

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

6. Roles/Responsibilities Defined

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

7. Definition of Critical Functions

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

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.
- Does the contingency plan address issues relative to pre-planned alternate locations? The contingency plan must address any potential issues relative to pre-planned alternate locations. These include:
 - insurance
 - equipment replacement
 - phones
 - utilities
 - security.
- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities should include:
 - prioritizing operations
 - identifying key personnel and how to reach them

- listing backup systems and where they are located
- stocking critical forms, blank check stock and supplies off-site
- developing reliable sources for replacing equipment on an emergency basis.
- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?
- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?
- Have temporary data storage sites and location of stored backups been identified?
- Is the frequency of file backup documented?
- Have the arrangements been made for ensuring continuing communications capabilities?
- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
- Is system, application and other key documentation maintained at the off-site location?
- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?
- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.
- Is the contingency plan stored off-site at alternate/backup locations? Copies of the contingency plan should be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the contingency plan that are stored in a private home must be protected from inadvertent access.

9. Required Resources

- Are the following resources for supporting critical operations defined and available for an emergency?
 - Hardware
 - Software
 - Communications
 - Data
 - Documents
 - Facilities
 - People
 - Supplies

- Basic essentials (water, food, shelter, transportation, etc.)
- Does the contingency plan provide for backup personnel? As the contingency plan is implemented, it is necessary to have additional people available to support recovery operations. The contingency plan should specify who these people are and when they would normally be called into action.

10. Training

- Is management and staff trained to respond to emergencies? Security training should include modules for management and staff relative to their roles for handling emergency situations.

11. Testing the Contingency Plan

- Is there a section in the contingency plan that addresses testing of the plan?
- Testing of the contingency plan should address the following topics:
 - Test Philosophy
 - Test Plans
 - Boundaries
 - Live vs. Walkthrough vs. End-to-End Testing
 - Test Reports
 - Responsibilities.

12. Contingency Plan Maintenance

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

13. Relationships/Interfaces

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

14. Attachments

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

A. Actions for Each Phase

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

B. Procedures

- Are there detailed instructions for:
 - responding to emergencies?
 - recovering?
 - restoring operations?
- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency should be in place.
- Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?
- Is there an implementation plan for working from home?

C. Call Trees

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

D. Hardware Inventory

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

E. Software Inventory

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

F. System Descriptions

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

G. Alternate/Backup Site Information

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

H. Assets/Resources

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

I. Risk Assessment Summary

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

J. Agreements/Memo of Understanding

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

K. Manual Operations

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

L. Supplies/Materials/Equipment

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

M. Floor Plans

- Are the necessary floor plans available?

N. Maps

- Are the necessary area and street maps available?

Appendix C

An Approach to Fraud Control

(Rev. 4, 03-05-04)

1.0 Introduction

2.0 Safeguards Against Employee Fraud

3.0 Checklist for Medicare Fraud

1.0 Introduction

(Rev. 4, 03-05-04)

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

2.0 Safeguards Against Employee Fraud

(Rev. 4, 03-05-04)

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

A. Screen New Employees

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

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

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

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

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

B. Bonding

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

C. Separation of Duties

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

D. Rotation of Duties

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

E. Manual Controls

Manual controls are differentiated from automatic controls because constant review is necessary to see that they are in place and working. Moreover, they often supplement or

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

F. Training

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

G. Notices

Notices, both periodic and situational, are effective and necessary in the prevention and control of fraud. It is not enough to formulate management policy, or to conduct employee training relative to fraudulent activity. It is possible to remind employees of management's continuing concerns and to evaluate employee awareness through simple reminders or announcements of what is happening relative to fraud controls (of a general nature) and management's reliance on their cooperation and understanding of their responsibilities. Without this evidence of sustained management commitment, policy

utterances tend to fade from memory or become regarded as part of a new employee's orientation and not part of the scene. This is true of minor abuses, but is also true of abuses that escalate into fraud.

H. Automatic Controls

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

I. Audit Routines

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

3.0 Checklist for Medicare Fraud

(Rev. 4, 03-05-04)

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

- 1) Have Medicare operations been identified where fraud or complicity in fraud may be possible, e.g. initiation/approval of payments?
- 2) Have individuals been assigned fraud-protection responsibilities in such components, including the responsibility for reporting possible fraud and vulnerability to fraud?
- 3) Do individual employees at **all** levels understand that management policy relative to fraud is dismissal and prosecution?
- 4) Are fiscal operations regularly audited relative to fraud vulnerability?
- 5) Are fraudulent acts specifically mentioned in the employee's code of ethical conduct?
- 6) Is employee integrity specifically addressed during the hiring process, and do background investigations elicit information that would uncover an applicant's past fraudulent activity with other employers?
- 7) Are operations set up in such a way as to discourage **both** individual and collusive fraudulent activity?
- 8) Are programs/systems tested by authorized individuals with "fraudulent" input?
- 9) Are audit trails generated *that* identify employees creating inputs or making adjustments/corrections that would pinpoint responsibility for any fraudulent act?
- 10) Is there an effective mechanism for detection/prevention of payments being purposely misdirected to employees, relatives, or accomplices?

- 11) Are new or changed programs specifically reviewed for fraudulent code by those responsible for production-run approval (persons empowered to review changes but not to make changes themselves)?
- 12) Are controls designed to **prevent** fraud, especially in those operations where large sums could be embezzled quickly?
- 13) Are all error-conditions checked for fraud potential?
- 14) Are balancing operations done creatively so that an embezzler could not hide discrepancies?
- 15) Are the official activities of all employees, at all levels, subject to independent review by different reviewers (i.e., not always by the same evaluator)?
- 16) Does management insist on integrity at all levels?
- 17) Has management announced that employee's work activities will be reviewed (in unspecified ways) for both the fact and appearance of integrity?
- 18) Do tape/disk library controls in fact prevent tampering with files/programs for fraudulent purposes?
- 19) Are alternative fraud controls invoked during emergencies?
- 20) Are suspected frauds investigated promptly and properly and are they thoroughly documented?
- 21) Are fraud audits conducted both periodically and randomly?
- 22) Are random samples taken of claims/bill inputs and checked back to their sources?
- 23) Does the Personnel department check the applicant's background, employment record, references, **and** possible criminal record **before** hiring?
- 24) Are badges, I.D. #'s, and passwords promptly issued **and** rescinded?
- 25) Is off-hours work supervised, monitored, or otherwise effectively controlled?
- 26) Are all employees required to take their vacations and are their replacements required to check over the vacationers' past activities?
- 27) Are the credentials of outsiders, such as consultants and auditors, checked out?
- 28) Is temporary help bonded, hired from reputable agencies, and their activities restricted to the tasks to be performed? (Same principle applies to employees temporarily borrowed from non-Medicare components.)
- 29) Are written procedures controlled and restricted to employees currently assigned the relevant duties?
- 30) Are special fraud controls specified for backup operations?
- 31) Are incoming checks, including returned checks, handled by two or more individuals in the mailroom and are such teams switched around so that the same people are not always working together?
- 32) Are blank checks and automatic check-signing equipment strictly controlled with a tamper-proof numbering mechanism?
- 33) Is procedure/program documentation relative to the payment process treated as highly sensitive data and safeguarded when superseded?

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

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

Appendix D (Rev. 3, 03-28-03):

Acronyms and Abbreviations

A

AAL	Authorized Access List
AC	Alternating Current
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

CAST	Contractor Assessment Security Tool
CCMO	Consortium Contractor Management Officer
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CFR	Code of Federal Regulations
CICG	Critical Infrastructure Coordination Group
CIO	Chief Information Officer
CMP	Configuration Management Plan
CO	Central Office
COMSEC	Communication Security
CMS	Centers for Medicare and Medicaid Services
CPU	Central Processing Unit
CSAT	Computer Security Awareness Training
CSIRC	Computer Security Incident Response Capability
CSR	Core Security Requirements
CSSP	Computer Systems Security Plan
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
DMERC	Durable Medical Equipment Regional Carrier
DOS	Denial of Service
DSL	Digital Subscriber Line

E

EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EF	Exposure Factor
E-mail	Electronic Mail
EO	Executive Orders

F

FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
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

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
IS	Information System
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Plan
IT	Information Technology
ITMRA	Information Technology Management Reform Act

L

LAN	Local Area Network
------------	---------------------------

M

MA	Major Applications
MBI	Minimum Background Investigation
MCM	Medicare Carriers Manual
MCS	Multiple Console Support
MDCN	Medicare Data Communications Network
MIM	Medicare Intermediary Manual
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	Procurement Office/ Project Officer
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
SII	Security/Suitability Investigation Index
SIRT	Security Incident Response Team
SISSO	Senior Information Systems Security Officer
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

SSL	Secure Socket Layer
SSM	Shared System Maintainers
SSO	Systems Security Officer
SSP	System Security Plan(s)
SSPM	System Security Plans Methodology
SSSA	Senior Systems Security Advisor

T

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TO	Training Office

U

UID	User Identification
UL	Underwriter's Laboratory
U.S.C	United States Code

W

WAN	Wide Area Network
------------	--------------------------

Appendix E: Glossary

(Rev. 4, 03-05-04)

Term	Definition
Access	<p>(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)</p> <p>(2) Opportunity to make use of an information system (IS) resource. (NSTISSI)</p>
Access Control	<p>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)</p>
Access Control Facility	<p><i>An access control software package marketed by Computer Associates International, Inc. (FISCAM)</i></p>
Access Control Software	<p>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 warning, or allowing access to all resources without warning regardless of authority. (FISCAM)</p>
Access Method	<p>The technique used for selecting records in a file for processing, retrieval, or storage. (FISCAM)</p>
Access Path	<p>(1) The path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc. (FISCAM)</p> <p>(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.</p>

Term	Definition
Access Privileges	<i>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)</i>
Accountability	The existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established. (FISCAM)
Accreditation	(1) The official management authorization for the operation on an application and is based on the certification process as well as other management considerations. (AISSP) (FIPS PUB 102) (2) A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (NCSC-TG-004)
Application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. (FISCAM)
Application Controls	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. (FISCAM)
Application Programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities. (FISCAM)
Application Programs	See Application.
Application System(s)	<i>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)</i>
Application System Manager	See Application Manager.
Asset	Any software, data, hardware, administrative, physical communications, or personnel resource within an ADP system of activity.

Term	Definition
Attack	<i>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)</i>
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (NSTISSI)
Audit Software	<i>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)</i>
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)
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)

Term	Definition
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: <ol style="list-style-type: none"> 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	<i>A lock with a key pad-like device that requires the manual entry of a predetermined code for entry. (FISCAM)</i>
Classified Resources/ Data/Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (NSTISSI)
Code	Instructions written in a computer programming language. (See object code and source code.) (FISCAM)
Cold Site	An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative computing location. (FISCAM)
Command(s)	A job control statement or a message, sent to the computer system, that initiates a processing task. (FISCAM)
Communications Program	<i>A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks. (FISCAM)</i>
Communications Security (COMSEC)	Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (NSTISSI)

Term	Definition
Compact Disc-Read Only Memory (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally read-only. (FISCAM)
Compatibility	The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are key to achieving compatibility. (FISCAM)
Compensating Control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions. (FISCAM)
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components. (FISCAM)
Compromise	An unauthorized disclosure or loss of sensitive defense data. (FIPS PUB 39)
Computer	See Computer System.
Computer Facility	A site or location with computer hardware where information processing is performed or where data from such sites are stored. (FISCAM)
Computer Network	See Network.
Computer Operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems. (FISCAM)
<i>Computer-related Controls</i>	<i>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)</i>
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.

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

Term	Definition
Contingency Plan(s)	<p>(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)</p> <p>(2) A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (AISSP) (FIPS PUB 11-3)</p>
Contingency Planning	<p>(1) The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. (ISSPH - Glossary)</p> <p>(2) See contingency plan. (FISCAM)</p>
Contractors	<p>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.</p>
Control Technique	<p>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.)</p>
Cryptography	<p>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)</p>
Data	<p>Facts and information that can be communicated and manipulated. (FISCAM)</p>
Data Administration	<p>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)</p>
Data Center	<p>See Computer Facility.</p>
Data Communications	<p>(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)</p> <p>(2) The transfer of data between functional units by means of data transmission according to a protocol. (AISSP) (FIPS PUB 11-3)</p>

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

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

Term	Definition
Dial-up Security Software	<i>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)</i>
Disaster Plan	See Contingency Plan.
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (FISCAM)
Disclosure (Illegal Access and Disclosure)	Activities of employees that involve improper systems access and sometime disclosure of information found thereon, but not serious enough to warrant criminal prosecution. These cases should be entered on the Fraud Monitoring and Reporting System.
Disk Storage	<i>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)</i>
Diskette	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case. (FISCAM)
<i>Electronic Data Interchange (EDI)</i>	<i>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)</i>
Electronic Mail (e-mail)	<p>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.</p> <p>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)</p>

Term	Definition
Electronic Signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. (FISCAM)
Encryption	The transformation of data into a form readable only by using the appropriate key held only by authorized parties. (FISCAM)
End User(s)	Employees who have access to computer systems and networks that process, store, or transmit information. This is the largest and most heterogeneous group of employees. It consists of everyone, from an executive with a desktop system to application programmers to data entry clerks.
Environmental Controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls. (FISCAM)
Exception Criteria	Exception criteria refers to batch processes that return files or records as not meeting certain predefined criteria for processing.
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)

Term	Definition
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. (FISCAM)
General Controls	The structure, policies, and procedures that apply to an entity's overall computer operations. They include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls. (FISCAM)
General Support System(s) (GSS)	<p>(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)</p> <p>(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)</p>
Guided Media	<p>(1) Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable)</p> <p>(2) Provides a closed path between sender and receiver</p> <ul style="list-style-type: none"> • Twisted Pair (e.g. Telephone cable) • Coaxial Cable • Optical Fiber <p>(Computer Assisted Technology Transfer Laboratory, Oklahoma State University)</p>
Handled	(As in "Data handled.") Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.
Hardware	The physical components of information technology, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. (FISCAM)
Hot Site	<i>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)</i>

Term	Definition
Image	An exact copy of what is on the storage medium
Implementation	The process of making a system operational in the organization. (FISCAM)
Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.
Information	(1) The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people. (FISCAM) (2) Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (AISSP) (OMB Circular A-130)
Information Resource	See Resource.
Information Resource Owner	See Owner.
Information Systems (IS)	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (NSTISSI)
Information Systems Security (INFOSEC)	The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including cryptosecurity, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (AISSP) (NISTIR 4659) (Also see Systems Security)
Information Systems Security Officer (ISSO)	(1) Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer. (NSTISSI)
Information Technology (IT)	(1) Processing information by computer. (TechEncy) (2) IT or Information Technology has probably been the most redefined term over the past few years. The definition has varied from simple automation of manual processes using micro-processors to computers to networks to desktop publishing to networking. (Source: U. Texas)

Term	Definition
Initial Program Load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program. (FISCAM)
Input	Any information entered into a computer or the process of entering data into the computer. (FISCAM)
Integrity	With respect to data, its accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users. (FISCAM)
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user. (FISCAM)
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)

Term	Definition
Junk Mail (e-mail)	Transmitting e-mail to unsolicited recipients. U.S. federal law 47USC227 prohibits broadcasting junk faxes and e-mail, allowing recipients to sue the sender in Small Claims Court for \$500 per copy. (TechEncy)
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message. (FISCAM)
Key Management	Supervision and control of the process whereby a key is generated, stored, protected, transferred, loaded, used, and destroyed. (NSTISSI)
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	<p>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).</p> <p>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)</p>
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	<p>(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.</p> <p>(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.</p> <p>(Source: ISO/IEC 12207)</p>
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)

Term	Definition
Load Library	A partitioned data set used for storing load modules for later retrieval. (FISCAM)
Load Module	The results of the link edit process. An executable unit of code loaded into memory by the loader. (FISCAM)
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)

Term	Definition
Maintenance	<p>(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)</p> <p>(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)</p>
Major Application (MA)	<p>(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)</p> <p>(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)</p> <p>(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)</p> <p>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.</p>
Malicious Software (Code)	<p>The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (AISSP – Source: DHHS Definition, adapted from NIST SPEC PUB 500-166)</p>

Term	Definition
Management Controls	<i>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)</i>
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)
<i>Master File(s)</i>	<i>In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period. (FISCAM)</i>
Material	Refers to data processed, stored, or used in and information generated by an ADP system regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements.
Media	The physical object such as paper, PC, and workstation diskettes, CD-ROMs, and other forms by which CMS data is stored or transported. The risk to exposure is considered greater when data is in an electronically readable and transmittable form than when the same data is in paper-only form. This is due to the greater volume of information that can be sent in electronic form, the ease and convenience with which the information can be transmitted, and the potential that such information will be intercepted or inadvertently sent to the wrong person or entity.
Methodology	The specific way of performing an operation that implies precise deliverables at the end of each stage. (TechEncy)
Migration	A change from an older hardware platform, operating system, or software version to a newer one. (FISCAM)
Minimum Background Investigation (MBI)	This investigation includes a NACI, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. The MBI is an enhanced version of the NACIC and can be used for selected public trust positions.
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)

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

Term	Definition
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)
<i>Operating System(s) (OS)</i>	<i>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)</i>
Operational Controls	<i>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)</i>
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy. (FISCAM)
Output Devices	<i>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)</i>
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. (NSTISSI)

Term	Definition
Penetration Test	An activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.
Peripheral	<i>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)</i>
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)

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

Term	Definition
Project Officer	CMS official (generally located in Central Office business components) responsible for the oversight of other business partners. These include Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased. (FISCAM)
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data. (FISCAM)
Public Access Controls	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records. (FISCAM)
Public Domain Software	Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances. (FISCAM)
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke Public key certificates accommodating a variety of security Technologies, including the use of software. (NSTISSI)
Public Trust Positions	Positions that have the potential for action or inaction by their incumbents to affect the integrity, efficiency, or effectiveness of assigned Government activities. The potential for adverse effects includes action or inaction that could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. (Source: 5 CFR Part 731)
Quality Assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures, and (2) the software meets the functional specifications defined by the user. (FISCAM)
Read Access	This level of access provides the ability to look at and copy data or a software program. (FISCAM)

Term	Definition
Real-time System	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed. (FISCAM)
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item. (FISCAM)
Recovery Procedures	Actions necessary to restore data files of an IS and computational capability after a system failure. (NSTISSI)
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior. (FISCAM)
Remote Access	The process of communicating with a computer located in another place over a communications link. (FISCAM)
Resource(s)	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and non-computerized records. (FISCAM)
<i>Resource Access Control Facility (RACF)</i>	<i>An access control software package developed by IBM. (FISCAM)</i>
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	<p>The potential for harm or loss is best expressed as the answers to these four questions:</p> <ul style="list-style-type: none"> 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?) <p>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)</p>

Term	Definition
Risk Analysis	<p>(1) The identification and study of the vulnerability of a system and the possible threats to its security. (AISSP – Source: FIPS PUB 11-3)</p> <p>(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)</p>
Risk Assessment	<p>(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)</p> <p>(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)</p>
Risk Evaluation	<p>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)</p>

Term	Definition
Risk Management	<p>(1) A management approach designed to reduce risks inherent to system development and operations. (FISCAM)</p> <p>(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)</p> <p>(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)</p>
Resource	Any agency Automated Information System (AIS) asset. (AISSP – Source: DHHS Definition)
Router	An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route. (FISCAM)
Rules of Behavior	Rules for individual users of each general support system or application. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training. (OMB Circular A-130)
Run	A popular, idiomatic expression for program execution. (FISCAM)
Run Manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. (FISCAM)
Safeguard	This term represents a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats. Safeguards are also often described as controls or countermeasures. (HISM)
Sanction	Sanction policies and procedures are actions taken against employees who are non-compliant with security policy.

Term	Definition
SDLC methodology	See System Development Life Cycle Methodology.
Security	The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability. (FISCAM)
Security Administrator (SA)	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks. (FISCAM)
Security Awareness	<p><i>(1) Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. (NIST SP 800-16)</i></p> <p><i>(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)</i></p>
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.
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)

Term	Definition
Security Management Function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness. (FISCAM)
Security Plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. (FISCAM)
Security Policy	The set of laws, rules, and practices that regulate how an Organization manages, protects, and distributes sensitive information. (NCSC-TG-004)
Security Profile	See Profile.
Security Program	An entitywide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. (FISCAM)
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (NSTISSI)
Security Requirements Baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security. (NSTISSI)
Security Software	See Access Control Software.
<i>Security Training</i>	<p><i>(1) Security training teaches people the [security] skills that will enable them to perform their jobs more effectively. (NIST SP 800-16)</i></p> <p><i>(2) Training strives to produce relevant and needed security skills and competencies. (NIST SP 800-50)</i></p>
Sensitive Application	An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (AISSP – Source: OMB Circular A-130)

Term	Definition
Sensitive Data	Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (AISSP – Source: OMB Circular A-130)
Sensitive Information	<p>(1) Any information that, if lost, misused, or accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. (FISCAM)</p> <p>(2) 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 (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (AISSP – Source: Computer Security Act of 1987)</p> <p>(3) 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 E-Mail 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987)</p>
Sensitivity of Data	The need to protect data from unauthorized disclosure, fraud, waste, or abuse.
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network. (FISCAM)
Service continuity controls	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (FISCAM)

Term	Definition
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)
Single Loss Expectancy (SLE)	<p>This value is classically derived from the following algorithm to determine the monetary loss (impact) for each occurrence of a threatened event:</p> <p>ASSET VALUE X EXPOSURE FACTOR =</p> <p>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)</p>
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)

Term	Definition
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
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	<p>(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)</p> <p>(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.</p> <ul style="list-style-type: none"> • The phrase "General Support Systems (GSS)" as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications (MA)," as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, control software, or software for command and control). By categorizing both "General Support Systems" and "Major Applications" as "systems", unless explicitly stated, the procedures and guidance can address both in a simplified manner. • When writing the required System Security Plans, two formats are provided--one for General Support Systems, and one for Major Applications. This ensures that the differences for each are addressed (CMS, System Security Plans (SSP) Methodology , July 2000, SSPM. • A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system's hardware may include mainframe systems, desktop systems (e.g., PC's, Macintoshes, laptops, handheld devices), workstations and servers (e.g., Unix, NT, NC), local area networks (LAN), and any other platform regardless of the operating system.
System Administrator	The person responsible for administering use of a multi-user computer system, communications system, or both. (FISCAM)
System Analyst	A person who designs a system. (FISCAM)
System Development Life Cycle (SDLC) Methodology	The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle. (FISCAM)

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

Term	Definition
Systems Security Coordinator (SSC)	Term used to designate the security officer in the 1992 ROM, MIM, and MCM. This business partner security officer had complete oversight and responsibility for all aspects of the security of the Medicare program.
System Security Officer (SSO)	The position held by the business partner Security Officer with complete oversight and responsibility for all aspects of the security of the Medicare program.
Systems Security Plan (SSP)	Provides a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (AISSP) (OMB Bulletin 90-08) (Also see IS Security Plan and System Security Plan)
System Security Profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS. (NSTISSI)
Tape Library	The physical site where magnetic media is stored. (FISCAM)
Tape Management System	<i>Software that controls and tracks tape files. (FISCAM)</i>
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	<i>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)</i>
Trap Door	A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with back door. (NCSC-TG-004)
Trojan Horse	(1) A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. (FISCAM) (2) A destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful. (AISSP – Source: Microsoft Press Computer Dictionary)
Unauthorized Disclosure	Exposure of information to individuals not authorized to receive it. (NSTISSI)
Uncertainty	This term characterizes the degree, expressed as a percent, from 0.0 to 100%, to which there is less than complete confidence in the value of any element of the risk assessment. Uncertainty is typically measured inversely with respect to confidence, i.e., if confidence is low, uncertainty is high. (HISM)
Unclassified	Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (NSTISSI)
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	<p>(1) The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM)</p> <p>(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)</p>
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	<i>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)</i>
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	<p>(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)</p> <p>(2) A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. (NCSC-TG-004)</p>
Vulnerability	This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. Both expected frequency (ARO) and exposure factor (EF) for fire are increased as a consequence of not having a fire suppression system. (HISM)
WAN	See Wide Area Network.

Term	Definition
Warning Banner	<p>NIST Special Publication 800-12 Footnote 131:</p> <p>The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. The ambiguity results from the fact that current laws were written years before such concerns as keystroke monitoring or system intruders became prevalent. Additionally, no legal precedent has been set to determine whether keystroke monitoring is legal or illegal. System administrators conducting such monitoring might be subject to criminal and civil liabilities. The Department of Justice advises system administrators to protect themselves by giving notice to system users if keystroke monitoring is being conducted. Notice should include agency/organization policy statements, training on the subject, and a banner notice on each system being monitored. [NIST, CSL Bulletin, March 1993]</p>
Wide Area Network (WAN)	<p>(1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM)</p> <p>(2) A communications network that connects geographically separated areas. (AISSP – Source: Microsoft Press Computer Dictionary)</p>
Workstation	<p>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)</p>
Worm	<p>(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)</p> <p>(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)</p>
Write	<p>Fundamental operation in an IS that results only in the flow of information from a subject to an object. (NSTISSI)</p>
Write Access	<p>Permission to write to an object in an IS. (NSTISSI)</p>

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://www.orim.nih.gov/policy.assip.html>, (for Source references see document)
4. Micki Krause and Harold F. Tipton, Handbook of Information Security Management (HISM), Imprint: Auerbach Publications, Publisher: CRC Press LLC, ISBN: 0849399475.
5. DoN - Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A, Aug. 3, 1982. (Glossary)
6. NSTISSI – National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999 (Revision 1)
7. TechEncy – Technical Encyclopedia of definitions supported by TechWeb.com

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