HCFA/Business Partners Systems Security Manual

Department of Health and Human Services (DHHS)
HEALTH CARE FINANCING ADMINISTRATION (HCFA)

Transmittal 1 **Date: January 26, 2001**

CHANGE REQUEST 1439

CHAPTERS	REVISED SECTIONS	NEW SECTIONS	DELETED SECTIONS
1-3	----------	ALL	----------
Appendix A-F	----------	ALL	----------

NEW/REVISED MATERIAL--EFFECTIVE DATE: January 26, 2001
IMPLEMENTATION DATE: January 26, 2001

This transmittal replaces the following:

Medicare Carriers Manual (MCM), Part 2 – Program Administration
Section 5135 – Systems Security Authority
Section 5136 – Systems Security Organization
Section 5137 – Contractor Systems Security General Administrative Measures
Section 5138 – Contractor Systems Security Specific Minimum Safeguards
Section 5139 – Exhibit: Physical Access to Medicare Areas
Systems Security - Appendix A: An Approach to Risk Analysis
Systems Security - Appendix B: An Approach to Contingency Planning
Systems Security - Appendix C: An Approach to Fraud Control

Medicare Intermediary Manual (MIM), Part 2 – Audits, Reimbursement, Program Administration
Section 2972 – Systems Security Authority
Section 2973 – Systems Security Organization
Section 2974 – Contractor Systems Security General Administrative Measures
Section 2975 – Contractor Systems Security Specific Minimum Safeguards
Section 2976 – Exhibit: Physical Access to Medicare Areas
Systems Security - Appendix A: An Approach to Risk Analysis
Systems Security - Appendix B: An Approach to Contingency Planning
Systems Security - Appendix C: An Approach to Fraud Control

Material in the above manuals and associated sections is being combined and replaced in their entirety. A reference page in the security sections of those manuals will now point to the recently developed HCFA/Business Partners Systems Security Manual (hyperlinks will be provided). Medicare Carriers and Medicare Intermediaries will now be required to follow the security requirements described in the new manual.

MAJOR CHANGES

The security sections of the MCM and MIM identified above, have been updated and combined into a new manual called the **HCFA/Business Partners Systems Security Manual**. The new manual is comprised of the following sections:

- Chapter 1 – Introduction
  This chapter provides an overview of the HCFA/Business Partners Systems Security Manual and references documents used to develop the manual, specifically Federal and HCFA mandates and guidelines for the handling and processing of Medicare data.

- Chapter 2 - IT Systems Security Roles and Responsibilities
  This chapter provides a description of the Consortium Contractor Management Officer (CCMO), the HCFA Project Officer (PO), and the Systems Security Officer (SSO). The roles and responsibilities of these entities are described in detail.

- Chapter 3 - IT Systems Security Program Management
  This chapter contains a program management planning table that will assist SSOs, managers with oversight responsibility, and other security staff in coordinating system security oversight activities at a business partner site.

- Appendix A: HCFA Core Security Requirements and the Contractor Assessment Tool (CAST)
  This appendix provides an overview of the Core Security Requirements, a hyperlink to an Adobe Acrobat (.pdf) file of the Core Security Requirements, and an overview of the Contractor Assessment Security Tool (CAST).

- Appendix B: An Approach to Risk Assessment
  This appendix provides a process to determine specific risks and corresponding safeguards that will mitigate the identified risks.

- Appendix C: An Approach to Business Continuity and Contingency Planning
  This appendix provides information on developing and implementing business continuity and contingency plans.

- Appendix D: An Approach to Fraud Control
  This appendix outlines specific safeguards against fraudulent acts by employees whose functions involve Medicare program funds.

- Appendix E: Acronyms and Abbreviations
  This appendix provides a list of commonly used acronyms and abbreviations.

- Appendix F: Glossary
  This appendix provides a list of commonly used terms and their definitions.

These instructions should be implemented as specified in Program Memorandum Intermediaries/Carriers, Change Request 1439.

Health Care Financing Administration (HCFA)
Business Partners
Systems Security Manual

HEALTH CARE FINANCING ADMINISTRATION
SECURITY AND STANDARDS
7500 SECURITY BOULEVARD
BALTIMORE, MD 21244-1850

January 2001

HCFA/Business Partners Systems Security Manual

Appendices

1. Introduction (Rev. 1 -- 01-26-01)

The Health Care Financing Administration (HCFA) 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 HCFA business partner is a corporation or organization that contracts with HCFA 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: HCFA Core Security Requirements (CSR), which provides the following:
    - An overview of the Core Security Requirements;
    - A hyperlink to an Adobe Acrobat (.pdf) file of the Core Security Requirements; and
    - An overview of the Contractor Assessment Security Tool (CAST).

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

- OMB Circular No. A-127, Financial Management Systems, February 8, 1996.
  http://www.whitehouse.gov/omb/circulars/a127/a127.html
- Presidential Decision Directive/NSC – 63 (PDD 63), May 22, 1998.
  URL to "White Paper: Clinton Administration's Policy: Critical Infrastructure Protection":
  http://www.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html
- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999.
  http://www.gao.gov/special.pubs/12_19_6.pdf
- HCFA System Security Plans (SSP) Methodology.
  http://www.hcfa.gov
- IRS 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, Rev 3-99
  http://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf

- Health Insurance Portability and Accountability Act (HIPAA), 1996. http://www.hcfa.gov/medicaid/hipaa/source/hipaasta.pdf
- HCFA Information Systems Security Policy Standards and Guidelines Handbook. http://www.hcfa.gov

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

- Department of Health and Human Services, Automated Information Systems Security Program Handbook (DHHS AISSP). http://wwwoirm.nih.gov/policy/aissp.html
- NIST Special Publication 800-3, *Establishing a Computer Security Incident Response Capability* (CSIRC), November 1991. http://csrc.nist.gov/ nistpubs/800-3.pdf
- NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, SP800-12. http://csrc.nist.gov/nistpubs/800-12
- National Archives and Records Administration Regulation 36 CFR Part 1228 Subpart K, NARA36 http://www.nara.gov/nara/cfr/cfr1228k.html
- Code of Federal Regulations, (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, PUB46-3. http://csrc.nist.gov/cryptval/des/fr990115.htm
- HCFA Internet Policy http://www.hcfa.gov/security/isecplcy.htm

HCFA Core Security Requirements will be updated periodically to reflect changes in these or other applicable documents (e.g., publication of final HIPAA rule).

2. IT Systems Security Roles and Responsibilities (Rev. 1 – 01-26-01)

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

The Consortium consists of four offices (Northeastern, Southern, Midwestern, and Western). The CCMO is a part of the Consortium and is responsible for HCFA contract management activities. CCMOs are responsible for the oversight of Medicare carriers and fiscal intermediaries. HCFA 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:

- HCFA 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 HCFA security policies and procedures.

2.2 The (Principal) Systems Security Officer (SSO)

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 can not have responsibility for operation, maintenance, or development. 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 HCFA Core Security Requirements by performing the following:

- Directing the Medicare IT system security program and assuring necessary safeguards are in place and working.
- Coordinating system security activities for all components of the organization.
- Budgeting for Information Systems Security.
- Reviewing compliance of all components with the HCFA 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 HCFA.
- 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 information 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 HCFA and external auditors.
- Cooperating in all official external evaluations of the business partner's systems security program.
- Conducting the (triennial) Risk-assessment (see Section 3.2).
- Ensuring that an operational Business Continuity and Contingency Plan is in place and tested (see Section 3.4).
- Documenting and updating the Corrective Actions Plan (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).
- Prearranging with the local fire department(s) safety control responsibilities for handling emergencies (see Appendix C).

3. IT Systems Security Program Management (Rev. 1 -- 01-26-01)

Business partners must implement policies, procedures, controls, or plans that fulfill the HCFA 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 these requirements and provides high-level descriptions of them. As appropriate, this section refers to other parts of this document that provides details on ways to accomplish each requirement. Business partners must perform a self-assessment using the HCFA Core Security Requirements. The supporting documentation, planned safeguards, and related schedules must be recorded using the Contractor Assessment Security Tool (CAST; see Appendix 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 HCFA 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)
A-2 Self-Assessment using CAST	Each Federal fiscal year	CCMO/PO with a copy to HCFA CO Systems Security Profile	See Appendix A, Section A-2, for an overview of CAST. Self-assessment results recorded using CAST are to be included as part of the Certification Package.	
3.1 System Security Plans	Each Federal fiscal year for each GSS and MA, or upon significant change	Systems Security Profile SSO	System Security Plans are to be reviewed and updated as necessary and are to be included as part of the Certification Package. More information about System Security Planning can be found in the HCFA SSP Methodology.	

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.2 Risk Assessment (Report)	Every 3 years or upon significant change	Systems Security Profile	Risk Assessments are to be included as part of the Certification Package. More information about Risk Assessment Reports can be found in Appendix B: "An Approach to Risk Assessment".	
3.3 Certification	Each Federal fiscal year	CCMO/PO with a copy to HCFA CO	Each year HCFA will issue a program memorandum (PM) on internal control certification. This PM will contain information on certification requirements including where, when, and to whom these certifications must be submitted.	
3.4 Business Continuity and Contingency Plan (Update){xe "IT Security Plans:frequency of updates"}{xe "IT Security Plans:responsibility for"}	Each Federal fiscal year, or upon significant change	Systems Security Profile	Management and the SSO must approve the Plan. Plans are to be included as part of the Certification Package and should be conducted in accordance with Appendix C: "Business Continuity and Contingency Planning". More information about contingency planning can be found in *An Introduction to Computer Security: The NIST Handbook* .	

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.5 Compliance	Each Federal Fiscal year	CCMO/PO with a copy to HCFA CO Systems Security Profile	There are two (2) components to compliance: **(1) Annual Compliance Audit:** Once a year, an independent audit will be performed on four (4) categories of the HCFA Core Security Requirements to validate the self-assessment. HCFA will determine the four categories the audit will validate by way of a Program Memorandum (PM). **(2) Corrective Action Plan** Corrective Action Plans address findings of annual self-assessments. CAST (see Appendix A, Section A-2) will record all items assessed as "Partial" or "Planned". The Corrective Action Plan is the set of all "Partial" and "Planned" items, along with their "Comments/Explanations" and "Projected Completion Dates."	
3.6 Incident Reporting and Response	As necessary	CCMO/PO Systems Security Profile	The HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file in the Security Organization	See HCFA SSP Methodology for additional information on the System Security Profile.	

LEGEND:

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

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

- **HCFA 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)

Business partners are required to maintain current Security Plans. Many of the other security requirements described in this Section are addressed in the IT systems security planning process or support the System Security Plan.

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).

Every system must have a System Security Plan, in accordance with the HCFA SSP Methodology, that documents its security posture as it is currently operating. The manager for the system or application is responsible for completing this document. The SSP documents the IT systems security process, which is described in the HCFA SSP Methodology. A System Security Plan is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. These plans should be distributed only on a need-to-know basis. The SSO receives the System Security Plan from the System Manager.

System Security Plans must be available to the CCMO/PO, the SSO, certifying officials, and authorized external auditors as required. A System Security Plan remains in effect until a new one is issued; however, the maximum time that may elapse before issuing a new (updated) plan is 3 years for each MA and every year for each GSS. The SSO is responsible for reviewing the SSP on an annual basis to ensure it is up-to-date. Standard System Maintainers are responsible for the System Security Plan (SSP) for their Major Applications (MAs) and General Support Systems (GSSs). Additionally, each business partner is responsible for documenting all unique items/details uncovered during the Risk Assessment process. Data Centers will be responsible to produce and supply the System Security Plans for all GSSs and MAs at the facility.

Business partners will attach a copy of the Standard System Maintainers plan when submitting their System Security Plan. Reviews for these plans are required at least every year or upon significant change, whichever comes first. If the system has changed so much that the current System Security Plan no longer describes the category of information, system or application, the system manager must update the plan.

3.2 Risk Assessment

Business partners are required to perform a triennial Risk Assessment (see Appendix B) and review it annually.

HCFA policy, as documented in Chapter 5 of the HCFA Information Systems Security Policy Standards and Guidelines Handbook, provides that all system and information owners must develop, implement, and maintain Risk Management programs to ensure that appropriate safeguards are taken to protect all HCFA resources. A risk-based approach should be used to determine adequate security and should 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. Appendix B, An Approach to Risk Assessment, should be used to prepare a risk assessment document. Additional information can be found in Chapter 4 of the HCFA SSP Methodology and in *An Introduction to Computer Security: The NIST Handbook*, Chapters 7 and 10.

3.3 Certification

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 HCFA 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 HCFA its IT systems security compliance within each Federal fiscal year. This security certification will be included in the annual internal control certification. HCFA 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 Appendix B),
- Business Continuity and Contingency Plan (see Section 3.4 and Appendix C),
- Results of Annual Compliance Audit (see Section 3.5), and
- Corrective Actions Plan (see Section 3.5).

Each year HCFA will issue a program memorandum (PM) on internal control certification. This PM will contain information on certification requirements including where, when, and to whom these certifications must be submitted.

3.4 Business Continuity and Contingency Plan

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

- Reviewed whenever new operations 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 C provides information on Business Continuity and Contingency Plans. The HCFA Information Systems Security Policy Standards and Guidelines Handbook, Chapter 11-Contingency Planning and Disaster Recovery, also explains with the contingency planning process and the reasons for establishing Contingency Plans.

3.5 Compliance

(1) Annual Compliance Audit

Each business partner must conduct an Annual Compliance Audit on four (4) out of the ten (10) categories of the HCFA Core Security Requirements. HCFA will notify business partners 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 HCFA Core Security Requirements.

Government auditing standards dictate business partner staff assigned to conduct an audit should possess adequate professional proficiency for the tasks required[1]. 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 HCFA. Required audit skills include proficiency in basic auditing tasks, communicating and project management.

An Annual Compliance Audit will have a verifiable information system security auditor assigned to coordinate the interviews, tests, 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.

(2) Corrective Action Plan

Medicare business partners must review their security compliance and determine the degree of compliance to the HCFA Core Security Requirements. The Corrective Action Plan addresses the risks identified as a result of the Annual Self-assessment and the Annual Compliance Audit (1). 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 HCFA 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 is the set of all "Partial" and "Planned" items, along with their "Comments/Explanations" and "Projected Completion Dates."

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

3.6 Incident Reporting and Response

An incident is the act of violating the security policy 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 Medicare data or the privacy of Medicare data. A reportable incident includes, but is not limited to, the following:

- Damage to the following systems;
- Contractor's own systems or operations
- Standard claims processing system
- Medicare Data Communications Network (MDCN)
- CWF host operation
- Compromise of system privileges (root access);
- Compromise of information protected by law (e.g., Federal Tax Information, Privacy Act data, and procurement sensitive data) whether in paper or electronic form;
- Denial of service of major Medicare IT resources;
- Malicious destruction or modification of Medicare data; and
- Identified successful intrusions.

Confirmed incidents are considered major risks and must be reported immediately to the CCMO. The CCMO should be kept informed of the status of the incident follow-up until the incident is resolved. The phone numbers for the CCMOs can be found in the contact address list in Section 3, above.

3.7 System Security Profile

Consolidate security documentation into a System Security Profile that includes the following items:

- Risk Assessment;
- Completed CAST Self Assessment(s);
- Annual Compliance Audit Report;
- Business Continuity and Contingency plans;
- Security reviews undertaken by DHHS OIG, HCFA, 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

Business partners are required to safeguard systems against fraud. The HCFA 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: HCFA Core Security Requirements and Appendix D: An Approach to Fraud Control.

3.9 Use of Medicare Resources in Private Business

Business partners are required to use Medicare data and resources in accordance with the Privacy Act. Information on an individual cannot be disclosed without the individual's written consent or except under limited circumstances, one of which is a "routine use", as specified in the system of records published in the Federal Register. "Routine use" permits disclosure of Medicare entitlement/payment information for the purpose of processing a Medicare claim under a "complementary plan". This "routine use" can be found in the Carrier Medicare Claims Record, System No. 09-70-0501, and in the Health Insurance Master Record, System No. 09-70-0502.

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

A-1 HCFA Core Security Requirements (Rev. 1 -- 01-26-01)

HCFA Core Security Requirements [Insert hyperlink to Core Security Requirements.pdf] detail technical requirements for business partners who use IT systems to process Medicare data. Business partners must establish and maintain responsible and appropriate safeguards 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 DHHS Office of Inspector General (OIG), and HCFA.

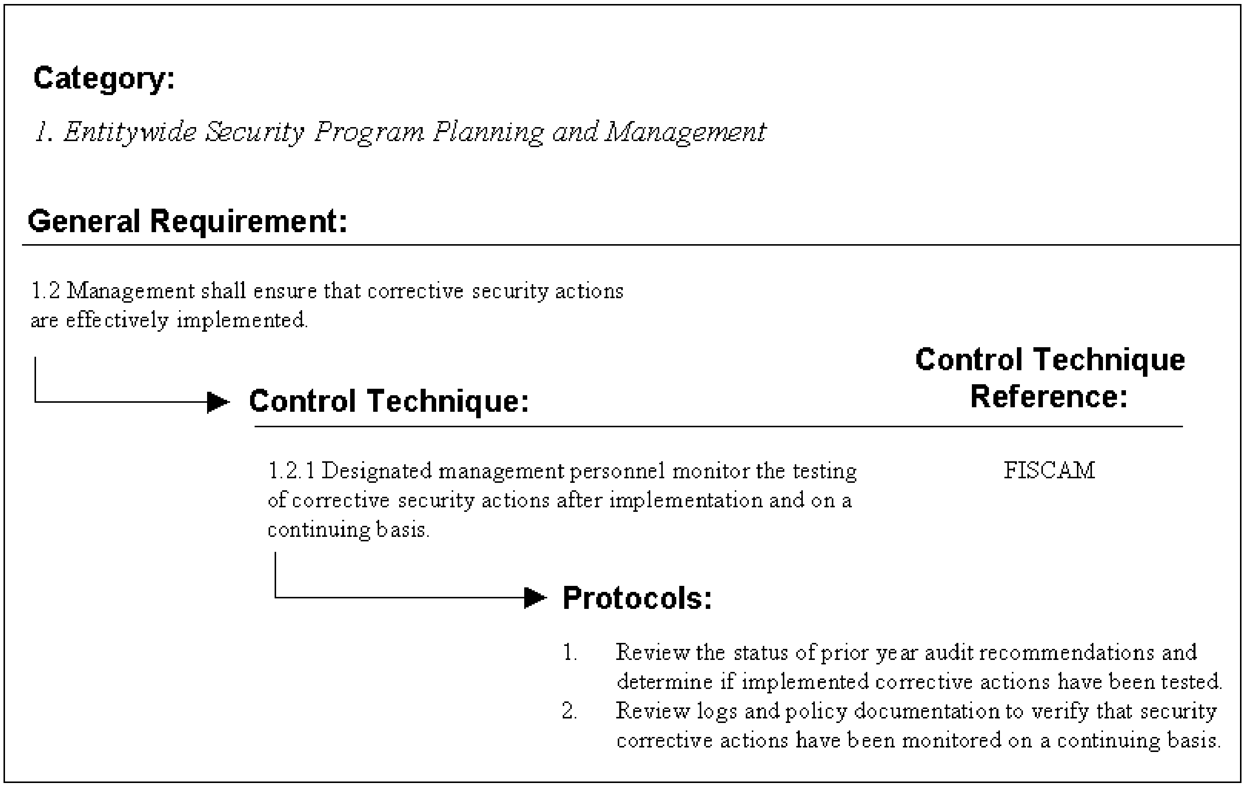
The HCFA Core Security Requirements were developed by assessing requirement statements from a number of Federal and HCFA mandates, including the following:

- OMB Circular No. A-127, Financial Management Systems, February 8, 1996.
  http://www.whitehouse.gov/omb/circulars/a127/a127.html
- Presidential Decision Directive/NSC – 63 (PDD 63), May 22, 1998.
  URL to "White Paper: Clinton Administration's Policy: Critical Infrastructure Protection".
  http://www.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html
- Federal Information System Controls Audit Manual (FISCAM), GAO/AMID-12.19.6, Undated.
  http://www.gao.gov/special.pubs/12_19_6.pdf
- HCFA System Security Plans (SSP) Methodology.
  http://www.hcfa.gov
- IRS 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, Rev 3-99
  http://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf
- Health Insurance Portability and Accountability Act (HIPAA), 1996.
  http://www.hcfa.gov/medicaid/hipaa/source/hipaasta.pdf
- HCFA Systems Security Policy Standards and Guidelines Handbook.
  http://www.hcfa.gov

HCFA 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 or damage. These controls are logical and 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 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 between General Requirements, Control Techniques, and Protocols.



Category:

1. Entitywide Security Program Planning and Management

General Requirement:

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

Control Technique:

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

Control Technique Reference:

FISCAM

Protocols:

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

Figure A-1. Relationship between 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 its business partners in this validation, HCFA 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 HCFA security documents used to create the HCFA Core Security Requirements and, as such, provide HCFA business partners with self-assessment procedures that are similar to audit procedures used by HCFA and external agencies.

Because HCFA 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.

Click the hyperlink below to download a copy of the HCFA Core Security Requirements in Adobe Acrobat (.pdf) format.

[Inset hyperlink to Core Security Requirements.pdf]

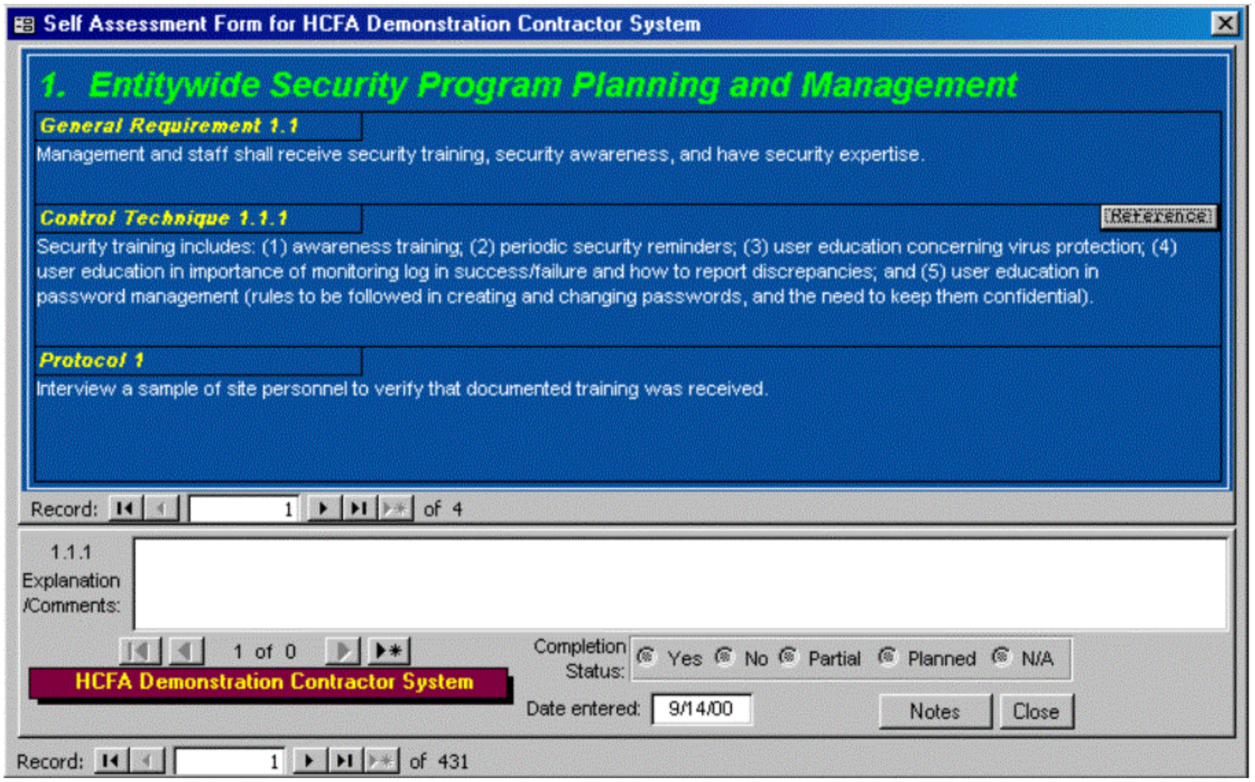
A-2 The Contractor Assessment Security Tool (CAST) (Rev. 1 -- 01-26-01)

HCFA will provide its business partners with the Contractor Assessment Security Tool (CAST). CAST is an automated database and software application that enables business partners to perform their self-assessments by entering data into electronic CAST questionnaires that are based on the HCFA Core Security Requirements and Protocols. The contractor will provide the CAST output as part of submitted certification material.

CAST provides business partners with a powerful reporting tool that generates formatted self-assessment forms, copies of HCFA Core Security Requirements, and standardized site-analysis reports. CAST also records information about a site, Risk Analysis schedules, and Contingency Planning schedules.

HCFA business partners can use the CAST Self-assessment form (Figure A-2 below) to conduct automated self-assessments. The CAST database includes Protocols designed to assess compliance with Core Security Requirements. HCFA requires that business partners complete annual self-assessments using CAST. The 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. CAST allows the business partner to generate a Q&A form that consists of those Core Security Requirements and Protocols that have a particular source document as a reference (e.g., IRS 1075, GAO FISCAM).

When entering information into CAST, the business partner will provide specific information in the Explanation/Comment field as to how they meet the requirement. CAST can then produce a formatted report of self-assessment results. CAST can also be used to analyze security data and output graphical analyses.


Self Assessment Form for HCFA Demonstration Contractor System
Reference
Record: 1 of 4
1 of 0
HCFA Demonstration Contractor System
Notes
Close
Record: 1 of 431

1. Entitywide Security Program Planning and Management

General Requirement 1.1

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

Control Technique 1.1.1

Security training includes: (1) awareness training; (2) periodic security reminders; (3) user education concerning virus protection; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential).

Protocol 1

Interview a sample of site personnel to verify that documented training was received.

1.1.1 Explanation /Comments:

Completion Status: ○ Yes ○ No ○ Partial ○ Planned ○ N/A

Date entered: 9/14/00

Figure A-2. CAST Self-assessment Form

Business partners are required to enter a comment or explanation for each self-assessment item of every status, as follows:

Yes - indicates that the systems or elements of operation conform to ***all*** aspects of the Control Technique. The Explanation/Comments field should contain:

- How exactly the Control Technique is met.
- What can be used to verify compliance.
- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.

Example Entry: *"Security Training is conducted during initial employees orientation and every year during the month of November for all employees and contractors. It includes all aspects outlined in the Control Technique as documented in company policy NG 7541-S3. The records of attendance are maintained by the corporate training office on the fifth floor of Bldg. #5 (cabinet #5). POC is Jim Socrates (401) 555-1212."*

No - indicates that the requirements of the Control Technique are not currently being met and there is no formal plan for meeting these requirements. The Explanation/Comments field should contain:

- Why this control technique is not being met.
- What is preventing corrective actions from going forward.

- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.

Example Entry: *"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) Green Hat (I. M. Programmer @ (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."*

Partial **-** indicates that the requirements of the Control Technique are not currently being met in their entirety. This can simply mean that one or more portions of a Control Technique are not being met. However, it is more likely that the requirements are being addressed and safeguards are implemented, but *not throughout the entire enterprise*. Enter a "Planned Completion Date" (required) and describe how the remainder of the system will be brought into compliance. Be clear and complete with these comments as this explanation with be part of the Corrective Action Plan as well as the Self-assessment submitted to HCFA. The Explanation/Comments field should contain:

- Why this Control Technique is not being met.
- What is being done to remedy the situation.
- Where applicable documentation can be found.
- Who is the principal point-of-contact for questions involving this requirement.

Example Entry: *"We use a mainframe and an offsite data storage facility connected via a T1 line and triple-DES encryption. However, the local corporate distributed network (WAN), which may house some administrative documents containing sensitive patient information, is connected via DSL and T1 lines to remote facilities without encryption. Network Encryption devices are currently on order. The POC in the security department is Iam Secure (401) 555-1234."*

Planned **-** indicates that the requirements of the Control Technique are not currently being met, but a plan of action exists to remedy the situation. Enter a "Planned Completion Date" (required) and describe how the system will be brought into compliance. The Explanation/Comments field should contain:

- Why this Control Technique is not being met.
- What is being done to remedy the situation.
- Where applicable documentation can be found.
- Who is the principal point-of-contact for questions involving this requirement. Enter a "Planned Completion Date" (required) and describe how the system will be brought into compliance.

Example Entry: *"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). The training POC is Jim Socrates (401) 555-1212. The POC in the security department is Iam Secure (401) 555-1234."*

N/A **-** The Explanation/Comments field for an N/A should contain:

- Why this Control Technique is not applicable.
- How you verified with HCFA.
- Where applicable documentation can be found.
- Who is the principal point-of-contact for questions involving this requirement.

Example Entry: *"This requirement describes required features of "security rooms". CSR 2.2.25 suggests "security rooms" as one 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 HCFA (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."*

CAST serves as the repository for the Corrective Action Plan (see Section 3.5 of the HCFA/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 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 HCFA/Business Partners Systems Security Manual).

CAST is available for download on the HCFA web site.

Appendix B:
An Approach to Risk Assessment

1. Risk Assessment: Getting Started (Rev. 1 -- 01-26-01)

The FISCAM defines Risk Assessment as 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. The primary goal of the risk assessment is to determine specific risks and the corresponding safeguards that will mitigate these risks. The overall risk assessment process will define the boundaries, allow for collection of information, and render a clear determination of the results through a risk analysis.

Risk assessment means figuring out what you have to lose and how likely it is you are going to lose it. If the risk is significant, you decide what to do about it. Can you reduce the impact of the loss? Can you reduce the probability that the loss will occur? What are the best safeguards? Are they worth the cost?

This may be simple in principle but not in practice. The risk assessment process may be subdivided into three steps, as follows.

Step 1: Determine Scope and Methodology

First, you have to figure out what to worry about. HCFA helps by categorizing the kinds of risks that could hurt Medicare assets and operations. HCFA also categorizes the assets, see Section 2. Wherever the assets are located, analyze the risks in terms of both the asset and related operations. For example, a workstation is a physical asset subject to risks such as fire and vandalism. See Section 3 for a description of the six main categories of risk. However, the operation of the workstation is also subject to risks such as fraud and error. HCFA categorizes safeguards into groupings more definitive than Administrative, Physical, and Technical; these three categories might be sufficient for the Privacy Act itself, but you need something more specific with which to work. There is a list of twenty different kinds of safeguards to consider when you get down to cases.

Step 2: Collect and Analyze Data -

Risk assessment requires, risk assessment experts working with operations experts, people asking questions and people answering questions. The proper mix is few askers, many answers. The ideal interviewer is well educated, self-motivated, imaginative, and knowledgeable in both systems security and Medicare operations. It takes awhile to develop the mind-set necessary to conduct a risk assessment so if you can not do the job yourself, restrict the number of interviewers, have them available for the duration of the risk assessment, and keep them on tap for future assessments. Your resident risk assessors are worth their weight in gold whatever the ounce is going for; although the full-blown risk assessment is done only once every 3 years, risk assessments are also done in connection with planning new systems and equipment installations. If you have your own staff, pick your brightest and educate them in risk assessment. If you have to borrow staff from Internal Audit, get one or two instead of ten or twelve and try for a long-term commitment; it is to your advantage to get the same talented person every time instead of having to train others.

Step 3: Interpret the Risk Analysis Results -

HCFA has provided matrices and worksheets to guide your risk assessment. Now you are trying to figure out whom to interview and how to conduct the assessment, so that the interviewers are not conflicting with one another. If there are two or three interviewers, coordinate their activities so that whoever talks to a particular individual covers all the risks and assets about which the expert is expected to know. Involving the operational area supervisor at the planning stage not only helps you but also makes clear that you respect his/her other commitments. With this approach, you may never hear an anguished, "But we've got work to do. "Sometimes you will have to call back to clarify a point or two, but you should not have to keep going back time and again to cover things overlooked the first time around.

Who are the interviewees? They are the people who to do the work, knowledgeable people, certainly, not somebody in training. They are people as close to the actual operations as possible, seldom higher than first line supervisors. Your risk assessment worksheet is the product of skilled questioning and the hands-on knowledge of the people who to do the work. Talk to them face-to-face, in their own operational areas, with only a worksheet between you. You want to see what is going on and you want to know what procedures are in practice. If your source does not know the answer to a particular question, someone in the area probably knows. Or, on the other hand, he might shrug his shoulders and say, "I haven't got the slightest idea. Why don't you try Jane Doe in Building Services?" (When you are through with this interview, look up Jane Doe.) Interview using the risk assessment checklist matrix and worksheet; when through, you want structured data that you can summarize for management action, not a jumble of facts and opinions that you have to massage for months in order to write conclusions.

Now that you know to whom you want to talk, how to do you get to them? Before you to do anything else, write a memo for the boss' signature (the higher the better) requesting a meeting of representatives from all pertinent organizational components at which you will preside.

When you meet with these organizational contacts, tell them what you hope to accomplish, how you plan to go about it, the levels of the workers with whom you want to speak, and when and where you would like to begin. You should have gone over the risk assessment matrices ahead of time, checking those risks that you and your HCFA contact feel are worth analyzing in each department. This gives each contact some idea of the scope of the risk assessment to be done. The contacts should then take the matrices back to their people to find out what additional risks should be looked into during the assessment. They also inventory their areas and write up functional statements of organizational responsibilities (all become part of the risk assessment package.) The contacts should be able to get back to you with completed matrices and firm schedules for filling out the worksheets. Cooperation is essential.

You are now able to talk, along with the contact, to anyone knowledgeable in an organizational component. There should be no adversary relationship. The proper attitude is that together staff and line are assessing risks. Bad marks come from missing something such as claiming fraud potential to be insignificant only to find two weeks later that the auditors have uncovered a million-dollar embezzlement.

Stage One - "Get Ready":

A good way to begin risk assessment is to go over a simple checklist with your initial contacts (and people you interview). A copy of this simple checklist is found below, and as Attachment 1 at the back of this manual.

MEDICARE RISK ASSESSMENT CHECKLIST

Building or Component Prepared By Date

Circle Code # if Condition Exists in Your Building or Component.

101 Building is old
102 Building has non-HCFA tenants
103 Building is in a high crime neighborhood
104 Building is in a tornado area or earthquake zone
105 Building is far from a fire station
106 Component has large electrical equipment/machinery
107 Component has highly burnable supplies, equipment, furniture, etc.
108 Component has false floors
109 Component is on the ground floor or lower and your building is in flood plain
110 Component is located on the top floor
111 Heavy equipment on floor above (or roof)
112 Equipment is old
113 Equipment requires air conditioning/climate control
114 Component has a sprinkler system or bad plumbing
115 Component is undergoing alterations/repairs (or will be shortly)
116 There is employee dissatisfaction or labor-management unrest
117 Data produced, used, or stored has value to others
118 Data could be used to defeat safeguards or exploit vulnerabilities
119 Data could be used to distort test results or gain unfair competitive advantage
120 Data might be material in legal actions
121 Data might embarrass the Medicare program or recipients if in wrong hands
122 Some employees are new and/or unaware of procedures
123 Some employees work under very tight schedules
124 Some employees eat, or drink in the component
125 Equipment/supplies are valuable, portable, and marketable
126 Equipment/supplies would be personally useful to employees or others
127 Strangers/customers/visitors are not unusual in the component
128 Component is near an exit opening on to street or parking lot
129 Equipment could be used on site to conduct non-HCFA business/hobbies
130 Operations involve disbursing/receiving payments
131 Emergency payments are common
132 Actual practices differ from official procedures

Your contact will be delighted to see that completing this simple checklist can be done by identifying the component to be assessed, showing who completed the checklist (the contact), dating the checklist, and circling the code numbers of conditions that indicate possible vulnerabilities. Your contact does not have to worry about the kind of risk to which the conditions relate. Even though it's not too hard to guess, for example, that circling code 125 (Equipment/supplies are valuable, portable, and marketable) indicates that theft of assets is something to think about when you get to the matrix which asks about significant risks.

Note that the first five conditions relate to the whole work location, not just the limited area of your contact's work site. An old building may not be as fire-safe as a new one, if for no other reason than that it may have been built before the current fire code was written. Because these general judgements affect all the areas, help your contacts out by giving them the answers. You will avoid the embarrassment of having differences of opinion from contact to contact relative to a condition that relates to the whole building. (Of course, there's nothing to stop you from getting their opinions and arriving at a consensus.)

Where you want differences of opinion is where there are differences. The rest of the conditions - codes 106 through 132 - refer to local conditions in the contact's component. True, machinery in one component (code 106) might increase the risk of fire for the entire building, but, chances are, something can be done in that component that can reduce the risk of a machine-related fire. Certainly, you will not expect a contact or interviewee to recommend area sprinkler systems for the entire building to reduce the risk of fire in his or her component. However, he or she might suggest that someone, somewhere along the line might be well advised to cost out a sprinkler system relative to fire risk for the entire building.

The time to refer back to completed checklists is when completing matrices and worksheets, then all one has to look at are items already circled. Those are the potential problem areas. Not that there has to be a special problem to warrant extra safeguards but the checklist red-flags special circumstances, highlights situations that call for a good, close, look before moving on to the next risk. Conversely, at matrix-time you and your contact will feel freer to move along when there are no circles on the checklist that relate to a particular risk, so long as there are suitable safeguards already in place and working.

All 32 of the checklist conditions are not explained, but each condition increases risks in some way. Heavy equipment on the floor above (or on the roof if the work area is on the top floor) could come crashing down in case of fire, or in case the roof-drain clogs in a rainstorm and tons of water add more stress to an already stressed roof. More confusing might be the inclusion of a sprinkler system, something you and everybody else rightly regard as a safeguard but coded here as a possible source of water damage should it go off accidentally or if there is no floor drain for the water.

You have just finished the "get-ready" stage.

Stage two - "Get Set":

The "get set" stage is collecting the information you need (possibly though preliminary interviews). Building maintenance, building security, and finance are good sources for preparing for interviews. Get set for your risk assessment interviews by gathering pertinent facts from your contact(s). You need cost data for the operational areas that you are to visit, cost of assets and cost of operations. Have your contact secure the figures so that you can calculate the amount that Medicare actually would be liable should the mishap occur; get insurance policies beforehand, including fidelity insurance, rental agreements, and contracts. What does a computer go for these days? Even though likelihood is speculative, you may be able to locate historical data on downtime and error rates. Loss is total recovery-cost, so go through contingency plans for the operational areas. They should be in the security profile. Contingency plans tell you what is involved in getting things back to where they were before the risk materialized.

Thorough preparation makes your job easier.

Risk assessment is far from exact, but it is wonderfully systematic and helps you and management lock a few barn doors while the horses are still inside.

Stage three - "Go":

You are ready for the "go" stage, which begins, with an inventory of the Medicare assets at risk.

2. Take an Inventory of Your Medicare Assets (Rev. 1 -- 01-26-01)

This means a physical inventory to see where everything is component by component. This is one job for the contact to do if you make clear what you want, and help estimate costs by supplying average prices for the kinds of equipment in the component. Get that information from budget people or whoever it is in your organization that keeps counts and lists of assets.

Medicare assets include whatever is used to process Medicare claims and bills. HCFA thinks of computers, terminals and workstations. The only way to get a handle on Medicare assets subject to various risks is to categorize them as to groups or separate them as the occasion demands. By and large, there are the seven categories listed below, with one category -Code 200 - that lets you lump all Medicare assets together for general risks such as fire and smoke that might effect the whole facility.

Code 200	All Medicare Assets (this includes everything listed below)
Code 210	EDP IT Systems and Data (storage media)
Code 220	Non-EDP IT Data (forms, documents, etc.)
Code 230	Computer Facilities (in the data center)
Code 240	Mini-Micro Computer Facilities (servers not in the data center but stand-alone)
Code 250	Remote Workstations and Links (PCs, terminals, etc.)
Code 260	Ancillary Facilities
Code 270	Other Medicare Assets (furniture, file cabinets, etc.)

These are the groupings on the matrix, so it's good to have your inventory arranged the same way within each component. Good, but not essential. Of course, not every component has every asset. Also coded and listed are the actual assets under each category. This defines the asset categories.

Code 210 EDP IT Systems and Data

This is computer data storage media plus input and output. It includes programs, and you don't have to treat each program or module as a separate entity, but as a system (code 218). Of course, "systems" includes both application systems and operating systems. Systems documentation (such as flow-charts and listings) belongs under 219 Other.

Code 210 is a general category of asset that includes the following:

211	Tapes
212	Disks
213	Other Magnetic and optical Storage media
216	Computer-Printed Output
217	Blank input/output Media
218	Systems
219	Other

Code 220 Non-EDP IT Data

Generally, this includes things not normally thought of as computer input or output. Once something is folderized you no longer think of it as computer output. Microfilm and microfiche are considered non-EDP; even those produced by a computer. All categories overlap; the important thing is to include the asset one place or another and not let it slip through the cracks.

Code 220 is a general category of asset that includes the following subcategories:

221	Source Documents
222	Forms and Letters
223	Microfilm
224	Microfiche
225	Claims Folders
226	Blank Forms and Letters
227	Written Instructions
228	Other

Code 230 Computer Facilities

This is pretty much everything in the data center. The CPU plus the peripherals, including any terminals. Site preparation is included here (raised floors, cables, temperature/humidity indicators etc.) because these are big expense items you might forget if you are not used to prying up floor panels on your inspection tours. Or pulling down ceiling panels. Or staring at the gauges on the walls. Other data center equipment could include transmission devices such as tape-to-tape, disk-to-disk, CPU-to-CPU, etc. The power and coolant distribution unit is added because experts tell us the big mainframes can't run without it. And memory is considered part of the central processing unit; the name for "cache memory" is "re-loadable control storage".

Code 230 is a general category of asset that includes the following subcategories:

231 CPU (includes main/buffer/cache storage) Microprocessor based server
232 Power & Coolant Distribution Unit
233 Computer Console/workstations

234 Auxiliary Storage (disks, RAID, etc.)
235 Mass Storage
236 Telecommunication Controllers; LAN Interface Devices, Hubs, Switches, and Routers
237 Tape/Disk Drives & Controllers
238 Other Data center Equipment
239 Site Preparation

Code 240 Mini-Micro Computer Facilities

Code 240 is a general category of asset that includes the following subcategories:

241 Workgroup Servers
242 Workstations
243 Stand-alone Minis
244 Remote Access Servers
245 LAN Hub, Switches, Routers, etc.
246 Other

Code 250 Remote Workstations/Laptops and Links

Remote access means potential access to everything on the computer.

Code 250 is a general category of asset that includes the following subcategories:

251 Input/output Devices, including printers, scanners, removable storage devices, etc.
252 Workstations, PCs, Laptops
253 Modems
254 LAN and direct local attachment links
255 Remote office routers with dialup capability
256 Dedicated remote connections
257 Other
258 Site preparation

Code 260 Ancillary Facilities

Code 260 is a general category for all those auxiliary facilities that support Medicare operations.

Code 270 Other Medicare Assets

Not to be confused with "All Medicare Assets", Codes 210 through 250, this category is limited to odds and ends that to do not rightly fit any place else. It was added because when the place burns down, the desks, chairs, and filing cabinets have to be replaced too. Nobody wants to do a risk assessment on a box of paper clips, but when you have general risks to worry about like those in the disaster and disruption categories you have Code 270 to stash things in. Maybe more importantly, now Code 200 for sure includes furniture and supplies along with everything else. (In any category of asset, small losses are automatically eliminated through your "significant risk" rule which rules out mishaps that don't amount to much annually in dollars lost, operations delayed, or records disclosed.)

Code 270 is a general category of asset that includes the following subcategories:

271 Office furniture (Desks, chairs, wastebaskets, etc.)

272 File Cabinets
273 Safes
274 Office supplies (Paper, pencils, paper clips, etc.)
275 Whatever doesn't fit any place else

3. The Matrix: A Shortcut to Risk Assessment (Rev. 1 -- 01-26-01)

Why not prepare a detailed risk assessment worksheet for every risk that might threaten every Medicare asset and operation? The answer is some risks do not pose significant threats and you would end up with a lot of unproductive paper work. (A blank matrix is provided at the back of this manual – Attachment 2)

A risk assessment matrix helps you associate risks with resources in a more general way. It lets you make judgments as to the seriousness of any threat, pre-judgments really, because you have not yet analyzed impact and probability. Using a matrix, you can dismiss further consideration of risks that obviously pose little threat to a particular asset or operation.

First, you make up a risk assessment matrix (Figure 3.1) for every component that has Medicare operations and assets. When you get through, you will have your whole organization covered.

Here is where your inventory comes in handy. Check to see which categories of assets are located in each component. Line out any column representing assets that are not in the particular component; in the example below, the heavy lines indicate that there are no big or little computers to worry about in the data entry component. This is how you tailor the matrix to show what kinds of assets are located in each component.

While looking at the sample matrix, look at all the risks listed down the left side. There are twenty-five specific kinds of risks that fall into six general categories: disaster, disruption, unauthorized disclosure, error, theft, and fraud. Assess risk at either the general category level or at the specific subcategory level. For example, ask yourself if more than one of the "Disaster" subcategories really does pose significant threats to the assets under consideration. If so, you may want to go with the general category, "Disaster." Unless, that is, you can see that possible safeguards will have little or nothing in common; a new roof to protect against storm damage is not going to protect against fire and smoke, and a new sprinkler system is not going to reduce the probability or impact of storm damage. When you get more used to the risk assessment process, such considerations will automatically come to mind during this preliminary assessment stage.

Five of the six main risk categories now include a subcategory of "Other" as the classical catchall. This way you know what to do with a Mt. St. Helens-type disaster even though there is no specific subcategory for volcanic eruptions. "Other Disasters" also accommodates such regional misadventures as mudslides, nuclear incidents, and the collapse of abandoned coal mines. HCFA is sure that there are more than four ways to defraud Medicare, so you now have an "Other Fraud" subcategory for the more inventive defalcators. "Unauthorized Disclosure," on the other hand, has no subcategories; this category automatically covers any kind of breach of privacy. It also covers improper disclosure of any other Medicare data determined to be sensitive, such as lists of customary and prevailing charges, fraud investigations, etc.

MEDICARE RISK ASSESSMENT MATRIX

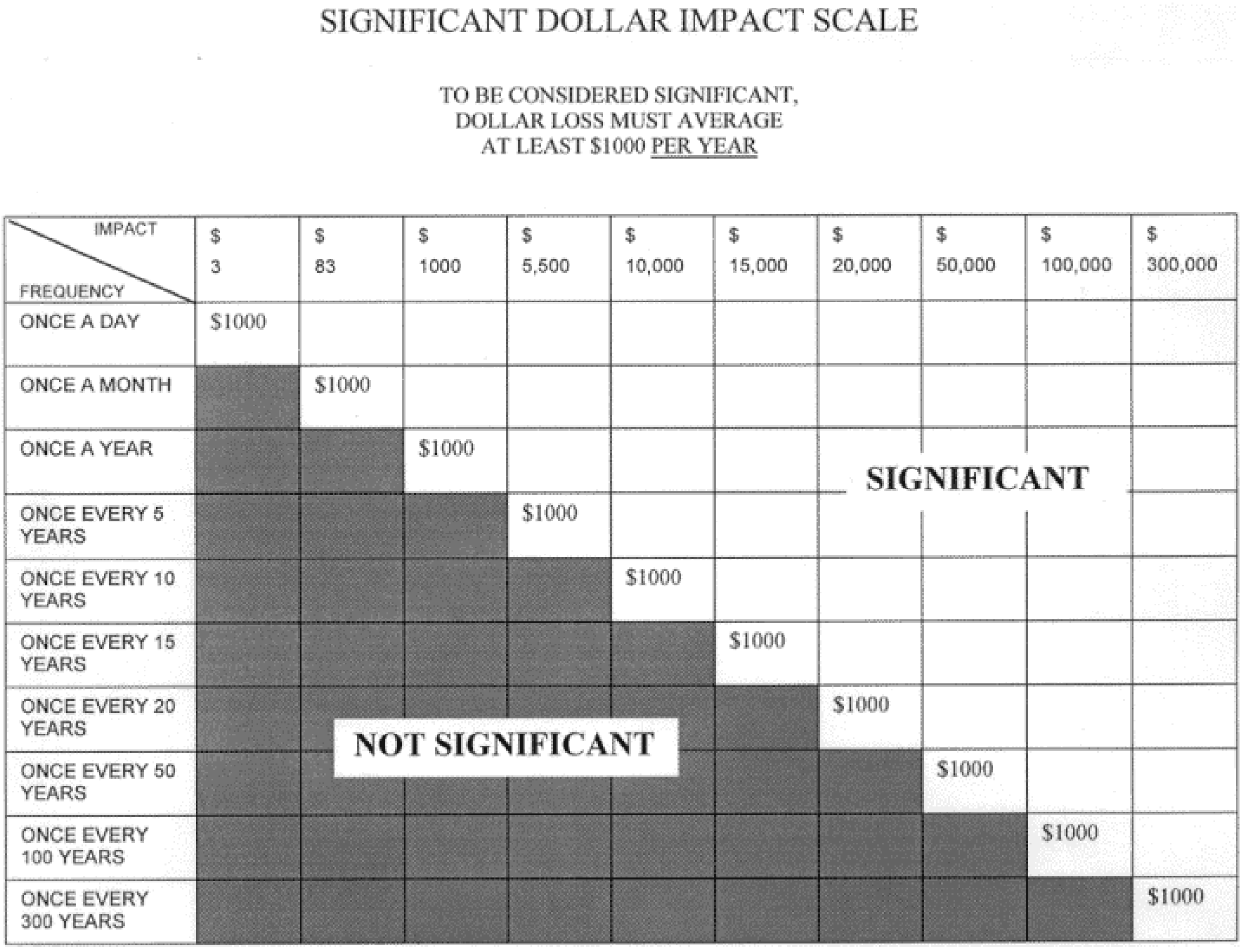
BUILDING OR COMPONENT: ____________________

▨	ALL MEDICARE ASSETS								
CHECK BOX ONLY IF YOU FEEL	▨	EDP Systems and Data							
THAT THE RISK MIGHT	▨	▨	Non-EDP Data						
AVERAGE OUT TO AT LEAST:	▨	▨	▨	Computer Facilities					
$1000 Net Lost per Year, or 2 Days	▨	▨	▨	▨	Mini-Micro Computer Facilities				
Delay Per Year, Or 10 Records	▨	▨	▨	▨	▨	Remote Workstations and Links			
Improperly Disclosed Per Year	▨	▨	▨	▨	▨	▨	Ancillary Facilities		
▨	▨	▨	▨	▨	▨	▨	▨	Other Medicare Assets	
	200	210	220	230	240	250	260	270	*Robert May* __________ 10/15/00 Prepared by Date
									PEOPLE TO BE CONTACTED
410 ALL DISASTER									
411 Fire and smoke									
412 Storm Damage									
413 Earthquake									
414 Explosions									
415 Civil Disorder									
416 Flood	X								*Harold Mandible*
417 Other Disaster(specify)									
420 ALL DISRUPTION									
421 Water Damage Other than Flood	X								
422 Vandalism/Sabotage						X	X		*Geri Ball*
423 Strikes and Job Actions									
424 Power Failure/Malfunction									
425 Air Conditioning Failure									
426 Heating Failure									
427 Machine Failure/Malfunction						X			*Lawrence Greer*
428 Other Disruptions(specify)									
430 ALL AUTHORIZED DISCLOSURE									
440 ALL ERROR									
441 Errors/Omissions		X	X						
442 Accidents									
443 Erasures									
444 Losing/Misplacing Assets									
445 Other Errors(specify)									
450 ALL THEFT									
451 Theft of Assets						X			*S. Proud*
452 Theft of Services						X			*S. Proud*
453 Other Theft(specify)									
460 ALL FRAUD									
461 Fraudulently Blocking Transactions									
462 Entering Bogus Transactions						X			*Jim McGlynn*
463 Altering Systems Programs						X			*Rafael Freeman*
465 Altering Records/Data Base									
466 Other Fraud(specify)									

Figure 3.1

A few paragraphs ago the term "significant risk" was used. Put a checkmark on your matrix when you think the risk is serious enough to warrant the completion of a risk assessment worksheet. (The next step.) One of the advantages of the matrix, it saves you from having to devote pages of rationale showing why a particular risk is not considered significant. You accomplish the same cull (elimination of insignificant risks) in no time at all simply by not checking a particular risk in relation to a particular asset/operation. If later challenged, you can always go back and to do a worksheet on that risk, but you certainly to do not have to go through that drill routinely for every risk, every asset. But to make this work-saver work for you, you have to understand that "significant risk" does not mean significant-per-incident but significant per incidence, meaning annual impact.

The scales below illustrate that "significant risk" is not merely impact, but impact multiplied by probability.



SIGNIFICANT DOLLAR IMPACT SCALE

TO BE CONSIDERED SIGNIFICANT,
DOLLAR LOSS MUST AVERAGE
AT LEAST $1000 PER YEAR

IMPACT / FREQUENCY	$ 3	$ 83	$ 1000	$ 5,500	$ 10,000	$ 15,000	$ 20,000	$ 50,000	$ 100,000	$ 300,000
ONCE A DAY	$1000									
ONCE A MONTH	▨	$1000								
ONCE A YEAR	▨	▨	$1000							
ONCE EVERY 5 YEARS	▨	▨	▨	$1000						
ONCE EVERY 10 YEARS	▨	▨	▨	▨	$1000					
ONCE EVERY 15 YEARS	▨	▨	▨	▨	▨	$1000				
ONCE EVERY 20 YEARS	▨	▨	▨	▨	▨	▨	$1000			
ONCE EVERY 50 YEARS	▨	▨	▨	▨	▨	▨	▨	$1000		
ONCE EVERY 100 YEARS	▨	▨	▨	▨	▨	▨	▨	▨	$1000	
ONCE EVERY 300 YEARS	▨	▨	▨	▨	▨	▨	▨	▨	▨	$1000

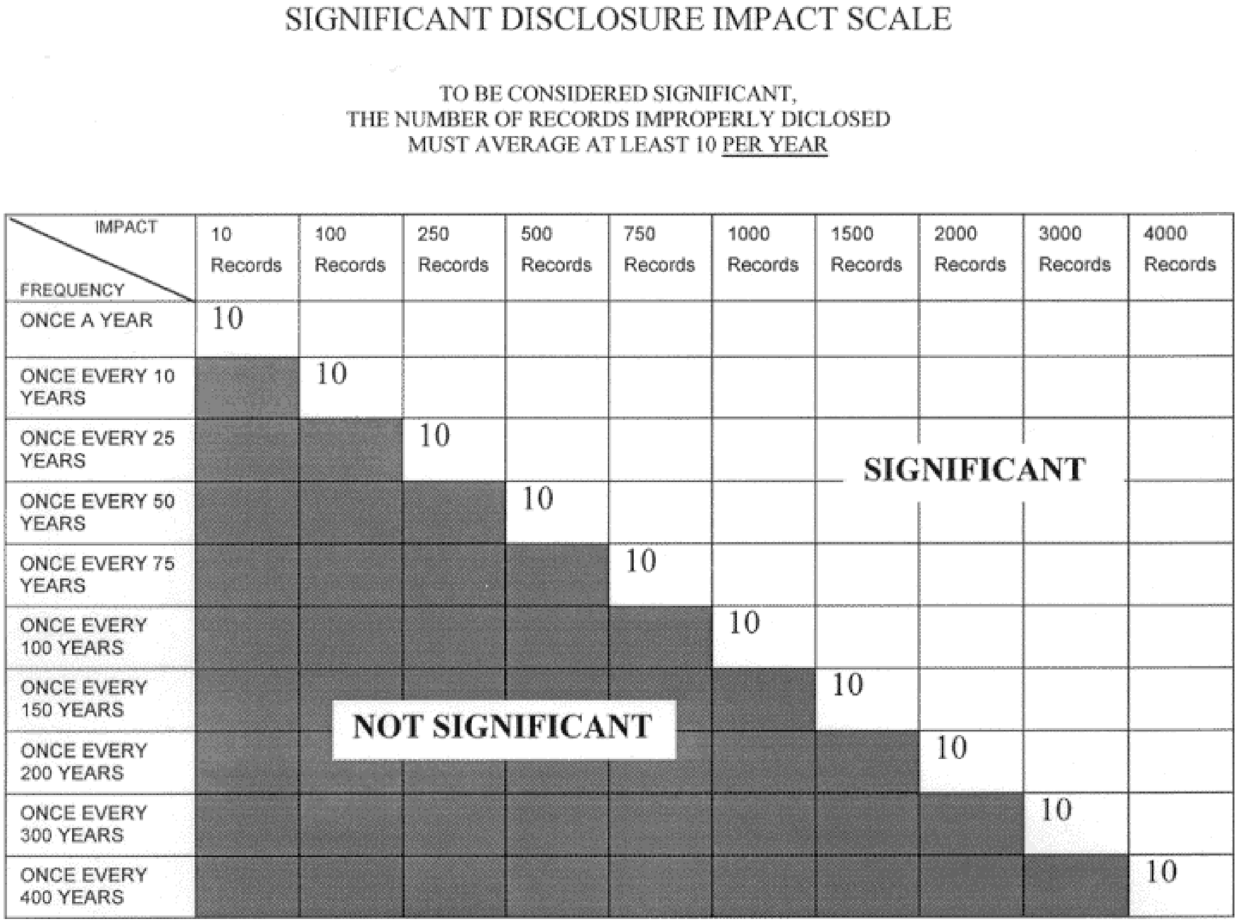
SIGNIFICANT

NOT SIGNIFICANT

Figure 3.2

This chart gives you a feel for "significance" when developing dollar estimates for your risk assessment matrix. For example, an impact estimated at $83.00 would have to happen at least once a month to be considered significant enough to warrant the preparation of a worksheet. (If it happened only once every 2 months or so, a dollar impact this size falls in the shaded area, a loss estimated at only $500 a year is not considered significant and the mishap should not be checked on the risk assessment matrix.) How likely would a mishap have to be before a loss of $110,000 would be worth worrying about? It would have to be considered likely to happen at least once in the next 110 years. Thus, even a large loss (impact) would not be considered significant if probability were low enough. Example; $110,000 divided by 150 years equals $770 Annual Impact Estimate, which would fade into the gray area of insignificance.

In case you are checking, yes, $3.00 is not strictly correct; to be significant, a daily loss would have to be only $2.75 to add up to $1,000 a year. Anyway you might have to translate this into a 5-day work week, or a 260-day year, which means you would have to be out at least $3.88 a day 5 days a week, 52 weeks a year before you would consider it.



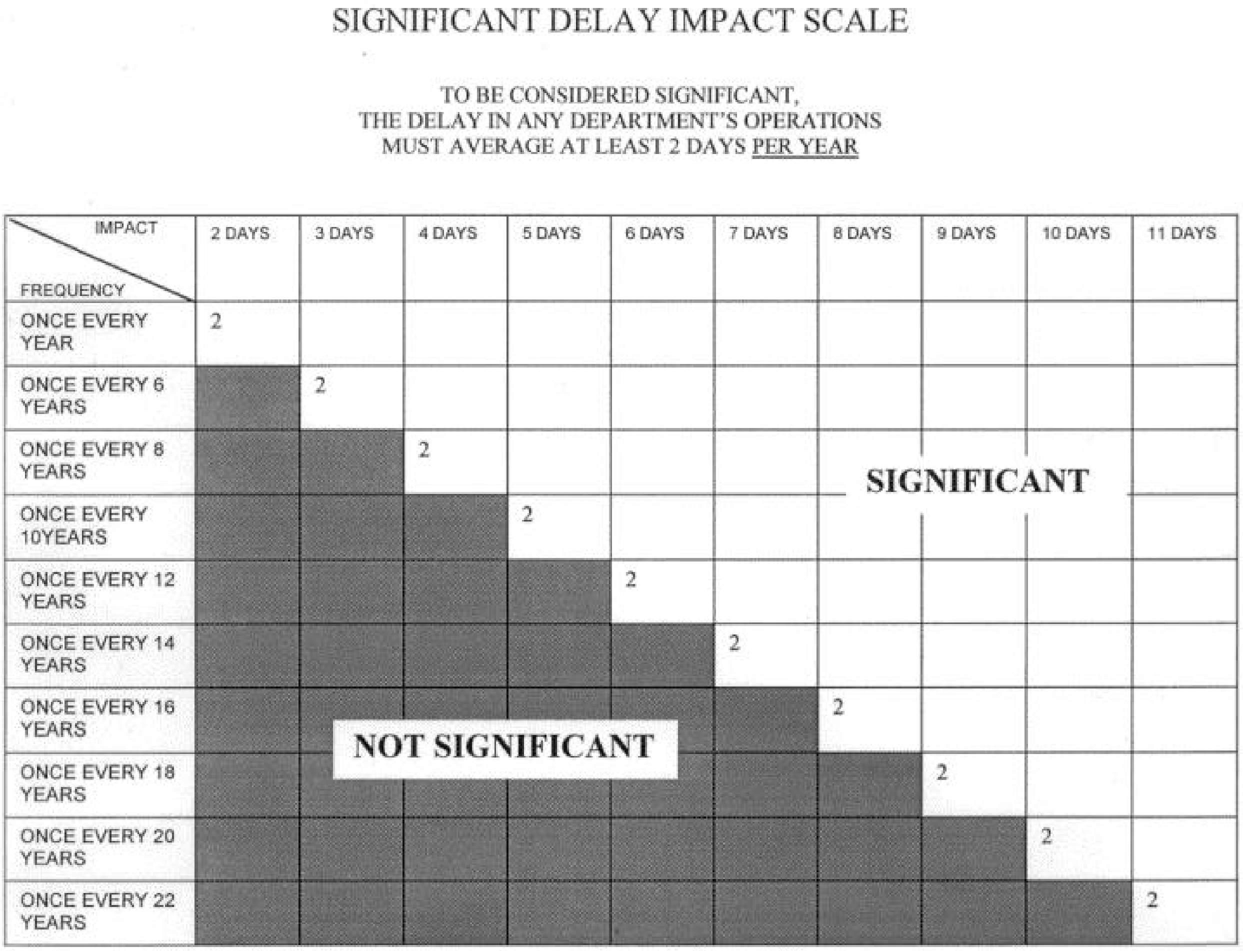
SIGNIFICANT DISCLOSURE IMPACT SCALE

TO BE CONSIDERED SIGNIFICANT,
THE NUMBER OF RECORDS IMPROPERLY DICLOSED
MUST AVERAGE AT LEAST 10 PER YEAR

IMPACT / FREQUENCY	10 Records	100 Records	250 Records	500 Records	750 Records	1000 Records	1500 Records	2000 Records	3000 Records	4000 Records
ONCE A YEAR	10									
ONCE EVERY 10 YEARS	▨	10								
ONCE EVERY 25 YEARS	▨	▨	10							
ONCE EVERY 50 YEARS	▨	▨	▨	10						
ONCE EVERY 75 YEARS	▨	▨	▨	▨	10					
ONCE EVERY 100 YEARS	▨	▨	▨	▨	▨	10				
ONCE EVERY 150 YEARS	▨	▨	▨	▨	▨	▨	10			
ONCE EVERY 200 YEARS	▨	▨	▨	▨	▨	▨	▨	10		
ONCE EVERY 300 YEARS	▨	▨	▨	▨	▨	▨	▨	▨	10	
ONCE EVERY 400 YEARS	▨	▨	▨	▨	▨	▨	▨	▨	▨	10

Figure 3.3

Ten-a-year is the level where the potential for improper disclosure is considered significant. Improperly disposing of a hundred records every ten years averages out to ten a year, indeed significant considering they might fall into the wrong hands. But if you projected a potential for improper disclosure of a hundred records less often -say once every l5 years, that falls into the shaded area where the risk is considered not significant, therefore acceptable; at least you don't have to drag it through the risk assessment process. Some personal records come in bunches - as on microfilm, microfiche, floppy, CDROM, or disk cartridge, so loss might be in units of hundreds or thousands, which is why the scale proves handy.



SIGNIFICANT DELAY IMPACT SCALE

TO BE CONSIDERED SIGNIFICANT,
THE DELAY IN ANY DEPARTMENT'S OPERATIONS
MUST AVERAGE AT LEAST 2 DAYS PER YEAR

IMPACT FREQUENCY	2 DAYS	3 DAYS	4 DAYS	5 DAYS	6 DAYS	7 DAYS	8 DAYS	9 DAYS	10 DAYS	11 DAYS
ONCE EVERY YEAR	2									
ONCE EVERY 6 YEARS	▨	2								
ONCE EVERY 8 YEARS	▨	▨	2							
ONCE EVERY 10YEARS	▨	▨	▨	2						
ONCE EVERY 12 YEARS	▨	▨	▨	▨	2					
ONCE EVERY 14 YEARS	▨	▨	▨	▨	▨	2				
ONCE EVERY 16 YEARS	▨	▨	▨	▨	▨	▨	2			
ONCE EVERY 18 YEARS	▨	▨	▨	▨	▨	▨	▨	2		
ONCE EVERY 20 YEARS	▨	▨	▨	▨	▨	▨	▨	▨	2	
ONCE EVERY 22 YEARS	▨	▨	▨	▨	▨	▨	▨	▨	▨	2

SIGNIFICANT

NOT SIGNIFICANT

Figure 3.4

Anything less than 2 days a year is not considered significant. Remember to forget about l-day delays no matter how often they happen each year. And remember that operational delays are being talked about, meaning the whole operation is out of order days-on-end; you are not asked to tally up the number of claims or bills delayed which could multiply out to thousands of days per year; don't deal in king-size years. Getting back to the scale, a 10-day delay every 5 years would average out to a significant 2 days per year, but a 10-day delay every 6 years would average out to something less and fall into the shaded area.

The same principles used to categorize risks are used to categorize Medicare assets. Some prefer the term "resources," others "assets." For the sake of manageability (and sanity) asset subcategories were omitted from the matrix. You should be able to risk out assets at this broad level for your broad-brush matrix estimates. If necessary, use the asset subcategories when completing the actual risk assessment worksheets.

Now let's look at the sample matrix again (See Figure 3.1) and the 25 kinds of risks that are listed. Your job is to relate each risk to the various Medicare assets and operations in that department. "Relate" means that you ask yourself if each risk poses a significant threat. Flood, for example, might pose a significant threat to all Medicare assets and related operations in the Data Entry Department if that department is located in the basement and your building is in a flood plain. (Risk assessment could be done floor-by-floor, but most risks are best analyzed department-by-department.)

Some risks will not relate to all Medicare assets and related operations, so check only those assets/operations that are threatened.

You may be able to treat some disaster-type risks on a whole-building basis, fire-and-smoke being a prime example. If so, head up one matrix for the building as a whole. Do not handle these risks department-by-department. If it turns out that this whole-thing approach is too cumbersome, you can always go back and relate the particular disaster to affected departments.

How do you decide whether a risk could significantly impact a particular Medicare asset or operation? Base your judgments on what you already know as a systems security expert, what you already know about your organization, and what you noted as you inventoried assets in each department.

Does the matrix burden fall on your shoulders alone? System security specialists for the CCMO are available to assist you. Once you are finished with the matrices, contact them and they will give you the benefit of their experience. The security specialist won't delete any of your checkmarks, but may suggest some. Then, there are your component contacts; they add any checkmarks you and the Regional Information Security Officer may have missed. Nobody deletes anybody else's checkmarks, but your contacts, being the operations experts in their own components, are certainly free to add their own.

When you've picked up the last matrix from the operating components you are ready to go, especially if the components have been nice enough to indicate whom you should talk to about each risk using the appropriate line in the appropriate space on the appropriate matrix.

The following should help you make your judgments as to whether or not a detailed risk assessment worksheet should be prepared.

When risk is used, it is risk to Medicare assets and operations, the asset plus the related operation. If an asset and operation are only 10 percent Medicare, it's that 10 percent to think about; a $5,000 total loss would be only $500 if Medicare is only 10 percent involved.

Is a $500 loss significant? Remember that $500 doesn't mean anything unless you know what time-span is involved. Risk assessment uses the annual 365-day year as a common denominator. So a $500 loss that occurs twice a year would mean a $1,000 annual loss. That's significant because for matrix purposes, losses of $1,000 a year or more are considered significant enough to warrant a worksheet (as are delays of 2 or more days a year, or disclosures of 10 or more records a year). Risk is loss times likelihood, something to keep in mind when developing your matrix estimates. Maybe a better way to put it is that risk is impact times likelihood, because that includes the money-less mishaps that substantially inconvenience or embarrass Medicare recipients.

You and your contact must sign and date each completed matrix. You don't sign until you get them back from each department and you are satisfied that they represent a fair sketch of your organization's security and the risks that deserve a closer look.

Risk categories on the matrix have been discussed. Pretty soon you are going to have a lot of specific questions. The six main categories of risk are:

- Disaster
- Disruption
- Unauthorized Disclosure
- Errors
- Theft
- Fraud

Except for unauthorized disclosure, these categories are too general to do much with. The following are sub-categories with which you can work.

A. Disaster

411 Fire and Smoke. Do you assume the whole building goes up in flames or do you assume limited fires, one floor and not another, one room and not another, one department and not another? Whichever way you go, the worst-case concept applies. Assume the worst damage that could reasonably result from any fire, considering the safeguards in place. On a whole-building basis, the sprinkler system in the stock room would reduce the likelihood of a fire that could spread to the rest of the building. Sprinklers or Halon in the data center would also reduce the impact of a general fire, unless the floor is likely to collapse and dump a million dollars worth of IT equipment into the fire. Fire spreads, smoke billows. Better housekeeping in the first floor mailroom may reduce the risk of losing your third-floor remote workstation, and everything else. If you decide to go the department-by-department route for risking-out fire damage, evaluate the far-reaching effect of any additional safeguards by using multiple-effect reckoning. Dollar damage is net - replacement cost less insurance - plus any other recovery costs such as overtime to catch up, or whatever it will cost to farm out work till you are back in operation, etc. If Medicare is 50 percent of your operation, the dollar loss is 50 percent of the total. Of course, Medicare suffers 100 percent of the delays.

412 Storm Damage. This indicates the kind of severe wind and weather damage from tornadoes, hurricanes, hailstorms, monsoons, freak ice storms, and sandstorms. Even snowstorms can be devastating; roofs collapse, transportation stops, firemen can't reach fires, and so on. Suffering is the key; do you suffer damage or delay as a result of the storm? Storm damage comes under disaster and this implies some kind of loss or interruption of operation, not just an exciting natural phenomenon. Handle rainstorms under flood, or in the leaky roof category, Code 421. Handle lightning here.

413 Earthquake. If you had 50 earthquakes a year, you would have no problem whatever estimating frequency and damage, but that's a high price to pay for ease of estimating. So what to do you to do if the earth quaked only once in anybody's memory, and then did no damage to speak of? You would forget it. But what if you know that earthquakes do happen occasionally in your locale and do damage? Check your "whole building" matrix at the All Medicare Assets

column unless expected damage would be significant only for some components. If you are located on the San Andreas Fault, you might be tempted to put a checkmark in that box despite lack of past damaging activity.

414 Explosions. Dust, Gas, Fumes, things do blow up from time to time. If you have gas heat in your buildings, and the drains back up when it rains, check it. If you can intelligently analyze this risk at the whole-place level, do it.

415 Civil Disorder. This doesn't seem to be a constant threat, and when peace and contentment prevail you can leave this line blank. You will know when to start worrying by listening to the news. Bomb threats belong here, not under explosions.

416 Flood. This is fairly predictable, being fairly memorable. (In Baltimore, Agnes in 1972 is famous as a flood even though the name technically belongs to a hurricane.) Flood damage can be based on past experience in the area, and chances are anything above the second floor can be considered safe. (Let us hope your computer isn't in the basement if you work in a flood plain.)

417 Other Disaster. This means whatever you want it to be, as long as it's spectacular enough. It should be something that doesn't comfortably fit into any of the disaster subcategories 411 through 416 already defined. Somewhere else mudslides and eruptions were mentioned as candidates for this "other disaster" category. Also you might want to include "aircraft crashes" if you have a heliport on your roof. You can list a dozen code 417s, as long as you specify what it is that could effect you. You should know what disasters are peculiar to your locale.

B. Disruption

421 Water Damage Other Than Flood. This includes leaky roofs, sweaty pipes, broken pipes, split water towers, dripping swimming pools (yes, some buildings have swimming pools on the roof and expensive computer installations beneath.) If your sprinkler system goes off prematurely this can cause problems as can unused pipes rusting slowly year after year, yet still not shut off. Personal experience for the building, plus your visual inspection should tell you whether to take this risk seriously enough to analyze further. This is the kind of risk that might affect one asset and not another, one operation and not another, so your whole-place matrix may be too broad. Your "All Medicare Assets" column may or may not be too broad.

422 Vandalism/Sabotage. If you find your terminals smothered in maple syrup, you know what vandalism is. Your place can be vandalized by outsiders breaking windows or stuffing a sprinkler hose through the mail slot on a long weekend. You or the people you talk to will know how much of a problem this kind of thing is for your organization and where it's happening. Sabotage is linked with vandalism because dirty work is dirty work and you hurt just as bad regardless of the motive of the wrongdoer.

423 Strikes and Job Actions. Things like slowdowns, sit-ins, sick-outs, and going-by-the-book can stop things cold. You will have to know if this is a common occurrence or if it's in the wind.

424 Power Failure/Malfunction. This is what some organizations spend lots of money avoiding by buying generators that cut in during outages. Power surges also play havoc with computers and if your system has been crashing a lot, now's the time to come to grips with the problem, start by checking 230 Computer Facilities.

425 Air Conditioning Failure. This refers to the effect on computers, which need to be kept cool to operate properly. It would have to be a hot spell and a long failure to affect other operations seriously enough to worry about. If air conditioning failure is due to power failure, handle it under power failure rather than air conditioning failure.

426 Heating Failure. History should tell you if you have a significant heating problem, but a talk with the building engineer wouldn't hurt. He may be patching up a worn out plant that should have been replaced 20 years ago. This is a chance to bring management's attention to a problem. Some areas of some buildings always suffer from inadequate heating in frigid weather, and loss of productivity may be more serious than anyone has been willing to admit. Everybody worries about disgruntled employees, and employees tend to get disgruntled when they're sitting there freezing. (It's not the ones who get mad that you have to worry about, it's the ones who get even.)

427 Machine Failure/Malfunction. This is generally the best-documented trouble you will come across. Downtime and repair costs are routinely recorded, and the records are routinely ignored in some organizations. Your job is to dig out the statistics and translate back into impact, and decide if it is significant or not.

428 Other Disruptions. These are those disturbances of peace and productivity not defined in Subcategories 421 through 427. They also should be incidents not showy enough to be thought of as disasters. A nice distinction would be those dusts and fumes in no danger of exploding but fully capable of corroding metal, or abrading moving parts, or shorting out electrical connections. It could be dirt from renovation or clean up of buildings in the area. Maybe the raised flooring tends to crumble as equipment is moved in and out of the data center.

C. Unauthorized Disclosure

430 All Unauthorized Disclosure. This probably should have been the number one risk; after all, the Privacy Act was inspired by the horrifying accessibility of personal data once it’s been computerized. Accessibility can be through remote workstations via dial-up and Internet. Removable media can be copied, so that pure data is stolen; nothing’s missing form the tape library except a person’s privacy. So who wants Medicare records? Somebody looking to get rich selling mailing lists that go for upwards of a quarter of a million dollars. Then there are some people who make a living out of tricking Medical reports out of hospitals and other health agencies for prospective employers who don’t want to hire someone disabled due to mental illness, or companies who don’t want to insure a bad risk, or other companies who want to sell supplementary medical insurance and need a leads list, or entrepreneurs who want to locate an eager market for terminal illness remedies. A selfish reason for guarding somebody else’ privacy is so people will trust you with current, accurate data; without this confidence, your data bank becomes unreliable. All Medicare personal data records have the sensitivity classification of Private (not top secret or secret or confidential or privileged) and this classification is the same for any utilization whether for appendectomy or alcoholism or drug addition or cancer or kidney failure or mental illness or emphysema, the information is nobody’s business who is not specifically authorized to get at it. Coinsurance is a legitimate and specifically authorized use of Medicare data, as is use of Medicare data by some agencies per contract with the Federal

Government. The point is, Medicare personal data can be properly used for those things specifically authorized.

D. Errors

441 Errors/Omissions. These are mistakes that cost billions of dollars a year, and for this reason alone must be included as possibly the major risk of doing business. Besides, an error-prone operation is an open invitation to fraud, and who wants to tempt an employee? Everybody likes to bury his mistakes, so you're going to have to interview people carefully and be super tactful in the way you report findings. (To do the job at all requires that the analyst be organizationally separate from the operational areas being poked into.) What you can look for with antagonism is the potential for error, something that does not sting like blame for past sins. Lean towards non-routine errors, the kind there's not already a procedure for handling. On the other hand, don't ignore gross error rates just because they've always been high and there is a staff of hundreds to correct them. Maybe your assessment will show you can catch mistakes earlier, before they have a chance to breed and multiply. When assessing your programming department, errors/omissions should make you think of program errors.

442 Accidents. This includes such diverse actions as spilling coke on the console, banging a forklift truck into a terminal, or pushing a cart full of magnetic tapes into an elevator that isn't' there. Unless you have an experienced safety engineer around who can point out hazards, you may have to rely on the experiences of the operating personnel. (And, of course, if the case has already been corrected, the risk may already be eliminated or greatly reduced.)

443 Erasures. This covers inadvertent tape or disk erasures and can be an annoyance or a disaster, depending on your backup. How to assess your organization's risk can be by experience or by the potential which you may discover by what procedures are used to prevent the thing from happening and how well the operator understands the procedures, and follows them. (Some operators have also managed to erase the backup tapes.)

444 Losing/Misplacing Assets. This refers to moveable assets like tapes and folders. Anything you can't lay your hands on when you need it. This risk's primary impact is in delays, but can also cost money in premature replacement or reconstruction. Losing a critical tape can effect your computer operation schedule. Although you don't have to worry about solutions at this point, tighter controls in the tape library are often indicated. This is a concrete example of how one risk can increase another.

445 Other Errors. These are those mistakes that don't belong in subcategories 441 through 444. If you have a problem that needs a niche not already supplied, use this "other error" subcategory.

E. Theft

451 Theft of Assets. This means somebody walks off with something. Computers are big but laptops are small enough to disappear. This category does not include theft of personal data, which comes under Unauthorized Disclosure. And it does not include theft of money, which comes under fraud. Impact depends on your loss potential. The loss is considered negligible if the equipment is adequately insured, but significant if the organization is going to have to stand

the loss. Other impact may be delay-pending-replacement. Or increased insurance premiums or increased rental costs attributable to the fact that the equipment was stolen from the premises.

452 Theft of Services. This can happen when some employee has a business on the side which he conducts using business partner equipment. Also included is charging computer time to Medicare operations.

453 Other Theft. This means theft of something other than assets or services. This is rather limited. Money and data are already covered elsewhere. If a dishonest thing happens that doesn't really fit anywhere else; maybe a pilferage problem that should be treated separately, and "Other Theft" might be the place for it. Besides, these dustbin subcategories serve a special purpose; when they're being used a lot, find out why and maybe add some new subcategories or redefine the old ones.

F. Fraud

461 Fraudulently Blocking Transactions. This is one of the simple ways to defraud an organization. Auditors look for unrecorded liabilities. Intercepting things like account corrections and adjustments can free up enough money to support a drug habit, etc. Look for money transactions where one trusted employee is allowed considerable scope; begging for trouble often succeeds.

462 Entering Bogus Transactions. This like payment for imaginary claims or bills may be the most popular method for defrauding an organization. Don't underestimate this risk potential; talk to the IT auditors and the regular auditors. Find out what controls exist, who's supposed to do what, and how things actually work. One employee (or several) can bankrupt a company. If you're looking for a way to justify risk assessment, tell management that their employees are engaged in risk assessment every day, even super-honest ones can't help noticing the opportunities for exploiting the system.

463 Altering Systems-Programs. This is what everybody worries about when they worry about fraud. And it just may be that this is the most successful way to defraud the organization, because programmers are fully capable of getting the computer to do anything they want, without anyone the wiser. How to assess the potential impact? History, if anybody will admit this having happened. Another way is to find out what programmer controls are in place, who authorized changes, who tests the controls, how much scope is allowed. In short, how much opportunity a person has to put the computer to work. Books on computer security show dozens of ways to keep programmers honest, and if the organization doesn't have at least a half-dozen in place, you're in trouble.

465 Altering Records/Data Base. This was meant to imply that both manual and computer records might be changed to create or divert payments. Computer crimes, for the most part, are the same old schemes adapted to computer technology. There's still plenty of potential for misdeeds in manual operations as well as in computers where payment is processed without human intervention. Medicare is claims-and-bills oriented, but there's also the potential for directly altering records without having to deal with current input.

Other Fraud. This identifies ways to cheat that don't involve the time-honored methods defined in the 461 through 465. It still deals with deceit and trickery and betrayal of trust, someone using his position to steal from (or through) his employer. Pilferage belongs under theft, not fraud. Money is usually the payoff for fraudulent activity rather than goods; even inventory is most often converted to cash and the cash diverted to the pocket of the perpetrator. Medicare doesn’t deal in goods and inventories, just money. Anywhere that an employee can use his duties or position, or scope of responsibilities to embezzle, is where there can be fraud. Other fraud could include things such as walking off with checks meant for somebody else undetected, which indicates some kind of effort to hide the fact that a crime has taken place.

4. How to Complete Your Risk Assessment Worksheets (Rev. 1 -- 01-26-01)

Go to each operational area with inventory, checklist and Medicare Risk Assessment Matrix in hand. Plus a few blank risk assessment worksheets (Blank worksheets come at the end of this material). The matrix shows whom to contact about each risk, supplied by the department head. Stress that your contact should be knowledgeable, not the individual most easily spared. Once you start interviewing, the worksheet is the only piece of paper you will need. This way all the facts and estimates you’ll need are structured and in a consistent format. The top three inches of the worksheet cover code numbers and "What-have-we-here?" type information. (See sample worksheet)

A. Name of Component

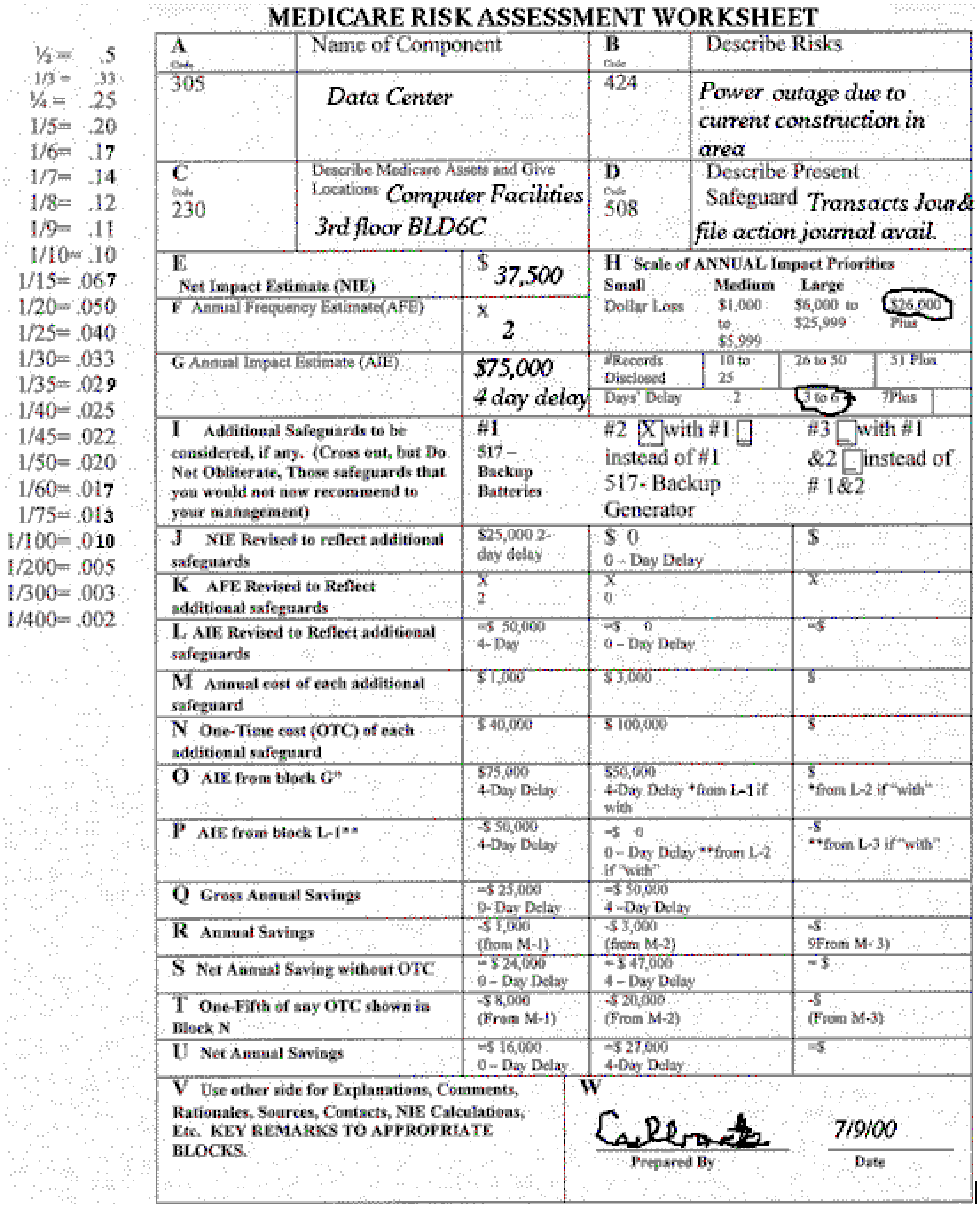
The matrix indicates where to go. What the description block calls for is the official name for the component. (In the example, it’s Data Center.) The code refers to the budget classification or cost center, 305 in the example (See the 300 codes below). Different people call different places different things, but the budget classifications are universal. The three-digit code tells the kind of Medicare operation the component is doing.

Code 300 All Medicare Operations. This covers the whole organization and is used for the big disaster-type risks that wreck everything.

301	Claims/Bill Review
302	Utilization Review
303	Hearing and Appeals
304	Data Entry
305	Computer Usage
306	IT Systems/Programming Support
307	Professional Relations
308	Service Department
309	Financial/Accounting/Statistical
310	General/Administrative
311	Medical Review
312	Provider Reimbursement
313	Provider Audit

If you don’t know what a particular category includes, you’ll find breakdowns in HCFA Intermediary Manual PUB 13-1 and HCFA Carrier Manual PUB 14-1. That’s the part called Fiscal Administration. Look under Budget Preparation.

One reason for being so explicit about where the asset is located organizationally is that different uses signal different risks. IT data in 305 is subject to different operational risks than IT data in 306. This was taken into account as each matrix was prepared and continued that concept in the worksheets.



½=	.5
1/3 =	.33
¼ =	.25
1/5=	.20
1/6=	.17
1/7=	.14
1/8=	.12
1/9=	.11
1/10=	.10
1/15=	.067
1/20=	.050
1/25=	.040
1/30=	.033
1/35=	.029
1/40=	.025
1/45=	.022
1/50=	.020
1/60=	.017
1/75=	.013
1/100=	.010
1/200=	.005
1/300=	.003
1/400=	.002

MEDICARE RISK ASSESSMENT WORKSHEET

A Code	Name of Component	B Code	Describe Risks
305	Data Center	424	Power outage due to current construction in area
C Code 230	Describe Medicare Assets and Give Locations Computer Facilities 3rd floor BLD6C	D Code 508	Describe Present Safeguard Transacts Jour& file action journal avail.
E Net Impact Estimate (NIE)	$ 37,500		
F Annual Frequency Estimate(AFE)	x 2		
G Annual Impact Estimate (AIE)	$75,000 4 day delay		

H Scale of ANNUAL Impact Priorities

	Small	Medium	Large	
Dollar Loss		$1,000 to $5,999	$6,000 to $25,999	[✓ $26,000 Plus]
#Records Disclosed	10 to 25	26 to 50	51 Plus	
Days' Delay	2	[✓ 3 to 6]	7Plus	

I Additional Safeguards to be considered, if any. (Cross out, but Do Not Obliterate, Those safeguards that you would not now recommend to your management)	#1 517 – Backup Batteries	#2 ☒ with #1 □ instead of #1 517- Backup Generator	#3 □ with #1 &2 □ instead of # 1&2
J NIE Revised to reflect additional safeguards	$25,000 2-day delay	$ 0 0 – Day Delay	$
K AFE Revised to Reflect additional safeguards	X 2	X 0	X
L AIE Revised to Reflect additional safeguards	=$ 50,000 4- Day	=$ 0 0 – Day Delay	=$
M Annual cost of each additional safeguard	$ 1,000	$ 3,000	$
N One-Time cost (OTC) of each additional safeguard	$ 40,000	$ 100,000	$
O AIE from block G"	$75,000 4-Day Delay	$50,000 4-Day Delay *from L-1 if with	$ *from L-2 if "with"
P AIE from block L-1**	-$ 50,000 4-Day Delay	-$ 0 0 – Day Delay **from L-2 if "with"	-$ **from L-3 if "with"
Q Gross Annual Savings	=$ 25,000 0- Day Delay	=$ 50,000 4 –Day Delay	
R Annual Savings	-$ 1,000 (from M-1)	-$ 3,000 (from M-2)	-$ 9From M- 3)
S Net Annual Saving without OTC	= $ 24,000 0 – Day Delay	= $ 47,000 4 – Day Delay	= $
T One-Fifth of any OTC shown in Block N	-$ 8,000 (From M-1)	-$ 20,000 (From M-2)	-$ (From M-3)
U Net Annual Savings	=$ 16,000 0 – Day Delay	=$ 27,000 4-Day Delay	=$

V Use other side for Explanations, Comments, Rationales, Sources, Contacts, NIE Calculations, Etc. KEY REMARKS TO APPROPRIATE BLOCKS.

W

Prepared By

7/9/00

Date

Figure 3.5

B. Describe Risks

The next thing to transfer from the matrix to the worksheet is the code number of the risk, code 424 is the example (Generally, prepare a separate worksheet for each check on the matrix.) Ask the contact if there is a better, more specific way to describe the risk. Is the risk peculiar to non-working hours? Do seasonal or peak workloads have an effect? Does the risk relate more to the assets or to the related operations? There's not much space to get a lot of information down, and the code itself suffices if nobody can think of a better way to shed more light. Code 424, for example, by itself indicates power problems, but "power outage due to current construction in area" indicates a temporary condition, and distinguishes the risk from power surges, etc. Make sure that someone else looking at the worksheet would understand what was recorded.

C. Describe Medicare Assets and Give Locations

Your matrix shows the general category of asset that each risk relates to, but you may want to get more explicit when completing your risk assessment worksheet. The example shows code 230 just like the matrix because power outages affect all the equipment in the data center. A more selective risk might have affected only certain equipment, in which case the appropriate subcategory would be shown for example code 233 indicating the computer console. For another example involving another category, code 210 on the matrix would indicate that the risk affects IT systems and data as a whole or one or more of Code 210's subclasses. Code 210 includes a lot of things, tapes, disks, etc. Verify with your contact if the checked risk threatens all such assets about the same, or only the ones actually located in the department. If so, use code 210.

But what if the risk threatens tapes only? Then use the 211 code for magnetic tapes.

Another possibility, what if the risk affects tapes and floppy disks only? Show codes 211 and 212. More than one code per block can be shown if the assessment can be handled on a single worksheet. Both assets can be handled together if both the causes and cures of the risk are the same.

Another possibility: What if the same risk threatens different assets in different ways? Say that the matrix is checked where errors intersect IT systems and data, but your expert tells you that significant errors involve only tapes and floppy disks. Okay, so far, but the causes are entirely unrelated and the possible safeguards will have little or nothing in common. The best way to go is to prepare one worksheet for code 211 and another for 212.

Another kind of possibility: not one specific asset, but several of them. For example, consider workstations. You have bunches of workstations in this department, but they are not all in the same place. Some are stationed out in the interview area on the first floor; some are located together in a lockable room on the second floor. Do you do a workstation-by-workstation assessment preparing a worksheet on each piece? Hardly. Or do you lump them all together? You could if the risk affected one workstation no more than another did. But if the risk is disclosure? Right away you see that the five workstations in the open pose more of a risk than the other five in a room that's out of harm's way; a room that gets locked up every night. In this example, you probably need a worksheet for the exposed workstations, none for the protected workstations.

The decision to lump or not to lump identical assets together is not that much of a problem. Or is not a problem that often, because you've already zeroed in on a particular risk in a particular operation for a particular asset and that narrows things down considerably. (Some of the company terminals are in different components, so you know you can't lump them together with the component terminals. On the other hand, by the time you do get to these other components you will have had considerable experience with terminals and should be able to use at least some of the facts you have developed.)

Since physical groupings have been talked about, and since this block calls for location of assets, don't forget to jot down your floors and room numbers and post locations, more than one address should your worksheet cover departmental assets at more than one location. Now that you and your operational expert have decided what to group with what, and where everything is at, it is time to figure that best way to describe the asset whose code you've already entered. You might want to ask our expert the following questions:

- How is the asset identified on the inventory?
- Does it have a brand name?
- Does it have a label?
- Exactly what does it do?
- What is its capacity?
- How many are we talking about?
- Are they all here?
- Are we expecting to get more shortly?
- Is site preparation necessary to this operation?
- What percentage of its use is for Medicare operations?

Looking at the modest space set-aside for description, you'll include only those things that actually help define the asset. If you need more room, continue the description in the space for comments on the back of the worksheet. In the example, computer facilities were called the asset, and the location indicated.

D. Describe Present Safeguards

One of the first judgments involved in risk assessment is: "What do we have going for us?" In some respects, this question is unanswerable. Often, the very way you do business determines how safe you are. What this space calls for is those evident, singular, identifiable, extraordinary things that are in place that reduce the impact of the risk or the likelihood that it will happen. Why bother listing present safeguards? To give some indication of your current protection and to give more meaning to any complementary safeguards you and your expert propose. Your expert is an operational expert, and he may not be fully knowledgeable of safeguards. Using the following list of safeguards, ask him which ones are in place in his department. Or elsewhere, if the safeguard helps reduce the risk in his department.

The code numbers generally identify the safeguard; any description should be explicit, showing how the safeguard relates to this asset/operation in this component. If you can, be brief; if you can't, write "see other side" in this block and elucidate the information on the back.

This list of safeguards is not a sneaky way to impose extra requirements. It's meant to give you a clear idea of what is in mind when the terms are used. Some safeguards may be appropriate to your situation, others may not.

Code 500 All Safeguards:

501 Policy
502 Procedure
503 Separating Duties
504 Training
505 Posters/Notices/Announcements
506 Testing/Validating/Editing
507 Audit Routines
508 Audit Trails/Journals/Logs
509 Alarms, Fire/Access/Etc.
510 Automatic Controls
511 Manual Controls
512 Good Housekeeping
513 Secure Disposal
514 Authorizing/Restricting Access
515 Relocating Operations/Equipment/Records
516 Modifying Building/Work Environment
517 Backup
518 Encryption
519 Insurance/Bonding
520 Maintenance/Repair/Replacement
521 Other (Specify)

NOTE: For practical purposes, general administrative safeguards are excluded from risk assessment. For example, risk assessment itself is something you do as part of your systems security program administration. It has to do with systems security but could hardly be described as "a safeguard." The same is true of all other program-type activities including contingency planning. To put a fine point on it, backup tapes could be considered a specific safeguard to reduce the impact of a specific risk, but the decision-making process known as contingency planning is much too nebulous to deal with in risk assessment.

501 Policy. This means the decision to do things a certain way, to announce an official course of conduct; policy is management's commitment to certain principles that are communicated to the staff for their guidance. Policy often takes the form of edicts and pronouncements. Like "Unauthorized attempts to circumvent controls will result in dismissal." Here, policy means the rules laid down by management to govern employees in the conduct of their duties so as to

minimize any of the six main categories of risk. Such policy decisions usually result in formal procedures, notices, announcements, etc.

502 Procedure. This implies a course of action or conduct that is written down for the use of the employee in performing his duties. Procedures tend to be fairly explicit, showing how certain jobs should be done. Procedures are often put in manuals; they are used as reference material, and as the authority for doing something in a particular way; written procedures are often included with training material for new employees. Stretch this to include structured programming, which is, after all, the procedure for computer processing. Systems security procedures should be based on systems security policy.

503 Separating duties. This does not mean trying to keep employees ignorant or confined to limited functions, but does mean that no employee should be allowed sufficient scope at any one time to defraud the organization. There is no reason not to promote an operator to programmer, but there is reason not to let an operator program the computer while also an operator, and there is reason not to let a programmer operate the computer. Cross-training is in no way a security violation (in fact, it enhances contingency planning and improves operations and morale.) Duties to be separated are altering programs; testing programs; authorizing program changes; and acting as custodian of tapes, disks and program documentation. Generally, a person who does a particular job should not be authorized to approve that same job, though it may be entirely proper to have a worker rotated to an authorization function, so long as it is someone else's work he is authorizing. Procedures such as structured program walk-throughs are excellent practice and require that several different individuals be involved in well-defined functions relating to the various stages in developing programs. Likewise, functions relating to paying/receiving funds should be arranged so that the functions and controls for any transaction are preformed by different employees.

504 Training. This can be formal or informal, but as a specific safeguard it refers to teaching employees specific things about how to do certain aspects of their jobs or how to operate certain equipment (such as fire extinguishers), or how to react in emergencies.

505 Posters/Notices/Announcements. These are ways to give employees specific information, as well as being consciousness-raising devices. Notices on security matters can be posted on employee bulletin boards. Announcements can be made over the loudspeaker system. Posters can be used in special areas to remind employees about specific security functions such as logging off the system when they are through transmitting. Signs are part of this scene when posted at entrances to areas containing sensitive data, saying "Authorized Personnel Only."

506 Testing/Validating/Editing. This covers routines meant to assure data integrity and the accuracy of new or changed systems/programs. This category excludes both audit routines and training-type activities such as fire drills. Reasonableness parameter testing also belongs here and not under "audit routines."

507 Audit Routines. This indicates devices designed to help the auditor check operations and data. These are generally software routines designed for specific purposes. Auditor programs can be used to produce a sampling of processed actions for auditor scrutiny, or to check certain accounts, or to extract file changes with input documents. This is a particularly useful audit device for on-line-file updating systems; such audit pinpointing is particularly suited to fraud

detection and day-to-day operational integrity. Any specific audit-type activity classifies as an audit routine (as opposed to annual internal audit of contractor systems security) whether the routine is through-the-computer or around it.

508 Audit Trails/Journals/Logs. These are records of transactions and who made them. The terms are used interchangeably and often include recording date, time, and location of the transaction, whether the transaction updates the file or is only a query. Journalizing makes it possible to analyze problems and to facilitate recovery in correcting or reconstructing files, regardless of cause. It is especially important in detecting perpetrators of fraud and privacy violations. Journals are computerized in on-line systems. Journalizing implies that the journal will be kept awhile and looked at occasionally for signs of fraud and error. Recording who-does-what fixes responsibilities; reviewing "signed" transactions brings wrongdoers to account and even has some preventive value. Especially when the safeguard is generally known to exist, though it's never wise to advertise how long you hang on to journal tape or what exactly is going to trigger a full investigation.

509 Alarms, Fire/Access/Etc. These include the obvious fire/smoke/burglar/water alarms, and also include any bell-ringing or light-flashing devices triggered by such things as repeated unsuccessful attempts to access the computer, or attempts to access off-limit areas or individuals, such as a receptionist, buzzing the guard office for assistance in handling unruly individuals. Alarms are meant to arouse somebody and inspire him to do something, so make sure that there will be people around who know how to respond before you install them. Think about nights and weekends and holidays and sickness and vacations. An alarm isn't an alarm if there's no one around.

510 Automatic Controls. These include things like sprinkler systems, even those time-delay systems that permit human intervention for a minute or two before the system activates. Lock-out of terminals at the end of the work day or response to unsuccessful attempts to penetrate computer/data base defenses is included, as are password protection, personal identifiers, selective terminal access to data bases through hardware/software controls, etc.

511 Manual Controls. These are devices that take care of the problem but must be operated by hand, such as wall-mounted fire extinguishers. (Training and practice in using manual controls is often implied, plus presence of someone to operate the device, plus alarms to alert the employee/guard.) Locks and safes are included under "authorizing/restricting access" rather than manual controls, as are the compiling and maintaining of authorization lists needed for limiting workstation users. Other major manual controls are sensibly situated switches (enhanced by posters/notices showing when they should be used, e.g., power-down procedures in data centers for various degrees of emergency.)

512 Good Housekeeping. This decreases the potential for fire, fraud, and unauthorized disclosure and assumes prompt, regularly scheduled, and proper disposal of things no longer in current use. Good housekeeping eliminates clutter, promotes order and a business-like environment. It means storing the least possible amount of supplies near operational areas, particularly computer areas. Cleaning products are forbidden to be stored in operational areas. Wherever they are stored it must be in a safe manner, i.e. oily rags in sealed metal cans, etc. Explosive dust (as from paper) is filtered out or cleaned out regularly, particularly from ducts,

and from under raised floors, and over lowered ceilings. Trash cannot be allowed to accumulate in or near buildings. Shredded paper is highly burnable and should be removed daily from the premises. Authorities agree that good housekeeping is one of the most effective safeguards available.

513 Secure Disposal. This means shredding, melting, cooking, boiling, chipping, etc., of any media containing personal data or sensitive information on Medicare program operations such as claims payment data. Retention schedules are often associated with secure disposal, and of course, the data is shipped and/or stored securely until destroyed.

514 Authorizing/Restricting Access. This includes creating and maintaining lists showing who is authorized in certain areas, and who is authorized to work overtime. Issuing badges, checking badges and revoking badges are all part of restricting access to sensitive operations or areas. Sign-in/sign-out sheets, guards, receptionists, locks, doors, windows, bars, grills, and safes are part of allowing only currently authorized individuals access to Medicare assets/operations. This category of safeguard does not include controls designed to restrict terminal access to computer files, matrix controls utilizing passwords, and personal identification numbers; such safeguards are included under "automatic controls."

515 Relocating Operations/Equipment/Records. This generally means getting them away from perceived risks, isolating them, regrouping, and rearranging to make it possible to secure them. Classic examples include moving computer operations out of basements that might flood, isolating public interview areas from Medicare claims processing operations, and moving terminals and their printers to rooms that can be locked (but providing doors and locks comes under "authorizing/restricting access"). Another example would be moving the tape library from over the cafeteria kitchen, or moving the kitchen out from under the library or moving all Medicare operations off the flood plain to a building high on a hill.

516 Modifying Building/Work Environment. This includes things like installing brighter lights, raising floors, enlarging air conditioning ducts (installing grills comes under restricting access), ripping out unused water pipes, replacing electric cable, installing washrooms in visitor areas, bricking up seventh floor data center windows against hurricane damage, etc.

517 Backup: Data/Power/Etc. This means storing duplicate program tapes and records in secure off-site locations. Even total redundancy in computer facilities would classify as backup, but contingency planning wouldn't. Even an arrangement for backup computer facilities would classify as backup because the arrangement is definite and specific; contingency planning on the other hand is too indefinite, too general to be considered a safeguard. The distinction can be illustrated using backup power as an example. For power outages, batteries and/or generators might be appropriate recommendations, but not for contingency planning. Asking the boss to consider contingency planning would be far too nebulous, like suggesting that somebody consider doing something about power outages. In short, contingency planning is an administrative initiative, not a safeguard. Contingency planning, like all administrative measures, is simply too all-encompassing to include in risk assessment; it works the other way around, risk assessment findings feed into contingency planning; you've got to estimate how serious something is before you can make appropriate plans. In our case, risk assessment comes

first before contingency planning even if the opposite were historically true and existing contingency plans generally influenced your risk assessment estimates.

518 Encryption. This means encoding and decoding data transmitted between a computer and another computer or terminal to prevent interception of intelligible data by tapping the interconnecting lines or cables. Because of the volume of data being transmitted back and fourth, an encryption system should use a unique key for each record. Privacy can be enhanced for stored data by having it encrypted so that stealing a magnetic tape file, for example, would not do the culprit any good. If encryption is indicated, it must be fully integrated with the rest of the system, thoroughly tested, rigorously controlled, and reckoned with in contingency planning. If not done with competence, encryption carries its own potential for disaster.

519 Insurance/Bonding. This should be looked into before a disaster strikes. Existing insurance may cover very specific and limited losses (fire but not flood, magnetic tapes, but not the data/programs stored on them). Rented equipment may be insured for certain things by the lessor but other disasters may be the responsibility of the Medicare contractor leasing the equipment. Some policies cover reconstruction of data files and may carry a $100,000 deductible, others may cover expected business revenue losses. Insurance should be considered in conjunction with other safeguards, particularly those reducing the likelihood of the mishap (such as good housekeeping practices) or those like backup tapes that also reduce a non-monetary impact such as delay. Bonding has kept many a trusting company from going down the tubes, but remember that somebody has to discover the fraud before you can collect. Medicare risk assessment is based on net loss, so you have to know what is covered and under what circumstances.

520 Maintenance/Repair/Replacement. This refers primarily to upkeep of equipment, the maintenance leaning toward preventive. Anything to keep your equipment from breaking down or to keep your building from falling apart. This is the kind of safeguard that minimizes the disruptive category of risk.

521 Other. This does not, repeat, does not include program-type activities such as annual audits, orientations, planning for contingencies, analyzing risks, etc. This category is restricted to specific remedies that do not fit in any of the categories 501 through 520. The specific safeguard should be identified by the individual using this category.

E. Net Impact Estimate (NIE)

A glance at the worksheet tells you it's dollar oriented. Dollar signs all over the place. The worksheet can and should also be used for things like disclosure and delay, but for now let's go with money.

Impact means how much it hurts each time it happens. In money, that is net loss. A $50,000 embezzlement is only a $40,000 net loss if bonding covers $10,000. That is why you looked up your fidelity insurance policies.

On the other hand, you want to include all costs associated with the risk. Replacement may be just part of the total recovery cost. For example, it might cost $7,000 net to replace a few workstations, but you might have to pay another $3,000 in overtime to catch up. Whatever percentage of this $10,000 is attributable to your Medicare operation is the amount that goes here in your NIE box. Show how such estimates are derived using the backside of the worksheet, otherwise who is going to know how you and your operational expert arrived at this figure? The NIE amount means little unless the people who have to use it can follow the computation. For example, the boss will want a breakdown to assure himself that you have thought of everything, and that this does represent only Medicare's percentage of the operation. Without your NIE calculations handy, management has to operate on blind faith. This requirement (justifying worksheet entries) will be referred to later, but this is an ideal place to strike a sensible balance between unsupported estimates and wordy rationalizations. Too many risk assessments turn into essays that philosophize endlessly about things having little or nothing to do with the risk. The worksheet is set up to quantify risk, to elicit figures. The back of the worksheet is reserved for explanations including breakdowns of whatever figures you come up with. Your NIE breakdowns should label all the individual expenses that add up to the total loss. Then come the deductions showing what to subtract for things like salvage, insurance, and that percentage of the total loss that is not attributable to Medicare operations.

Impacts are easily calculated for high frequency impacts; if the thing happens a lot, all you have to do is look up the records or get your expert to search his memory. It is when you are trying to come up with NIE for things that seldom happen that you start losing your bearings. This is where you use the worst-case concept. This is not Murphy's law, but merely a way to assume the worst that could reasonably happen should the risk materialize. All this sounds fairly straightforward, and it is, for things like fire and flood. Even for things like accidents and erasures and theft of services. But what is a reasonable worst-case impact for code 462, for example? If someone does enter bogus transactions, how much does he make off with before he is exposed? Will he ever get caught? It's not quite so hopeless as it seems at first. Considering your present, existing, in-place safeguards, what is the longest it could take to catch the culprit? Could others be doing the same thing? It is a guessing game sometimes. It gets you thinking. And it is entirely possible that someone will run across an actual embezzlement-in-process while doing a risk assessment. Isn't that exciting? But your job right now is to put a price tag on whatever mishaps might/could happen.

Let's say that every couple of months somebody tucks a printer under each arm and heads for the door. The impact per incident is whatever it costs for suitable replacements less whatever your insurance pays. No estimates needed here; if it happens often you go by experience. But what would it cost to replace a monitor, or a tape drive, or any of the other expensive equipment? If budget cannot give you replacement costs, try one of those big buyers' Bibles put out by private companies pricing IT equipment. Or call up your supplier and ask for quotes, just do not get his hopes up for a quick sale. Replacement cost is what it is going to set you back to replace what you have lost, less your insurance. You cannot say your have lost nothing simply because a perfectly good machine was fully depreciated. You might spring for brand new replacement, but if you could get an equivalent machine that works as well as the old one, that is your starting figure, your final figure being what you would have to shell out over and above your insurance check.

What if it would take you 3 weeks to get a replacement, meaning a 3-week delay in Medicare operations? You would use part of your impact space for delay. Use days, twenty-one days in this case. What if it is not money at stake, but privacy? Same space: Impact Estimate. Put down

100 records, if that is how many could get away from you at any one time. Maybe even once in a while printouts with Medicare personal data get thrown away without shredding. By mistake or on purpose, the point is unauthorized eyes may see records they should not. The average number per occurrence is the figure you estimate and enter. That is the impact, but you won't really know how serious it is until you start estimating frequency of occurrence. One final word about estimating delays; you are estimating operational delays, meaning the component cannot function, not delays in processing individual claims and bills.

Did you do your homework before you started interviewing? Did you review contingency plans? If not, how do you know what it would take to recover from disasters? There is more to destruction of your computer than just the cost of your equipment. You have to figure the cost of getting back into operation again. This may already have been done in your organization's contingency plan. If there is a contingency plan but no cost data, you can probably get the figures from Budget. (Ideally, you should do your contingency planning after you do your risk assessment, at least be prepared to modify those plans that may not be cost-effective according to your risk assessment.) If your tapes are backed up offsite, you only have to figure the cost of duplicating and transporting them. If you have only microfilm hardcopy documents stored offsite, you have to figure the cost of getting hardcopy. These are the kinds of things you cost out, item by item, on the back of the worksheet.

These are the kinds of questions that might need answering before you can estimate impact:

- What is the worst damage that could reasonably result from this risk relative to this asset and operation?
- What would repair costs likely be?
- If the asset would have to be replaced, what would be a likely replacement cost?
- Would any extra personnel costs be involved? Overtime, part-time help, or farming part of the work out?
- Is money involved, cash, checks?
- Are related costs involved, like site preparation?
- How much is covered by insurance or bonding?
- What would it cost to restore the asset or operation to where it was before the mishap?

F. Annual Frequency Estimate (AFE)

Here's where you put on your turban and bring a spare for your expert. You're both going to be forecasting events. The easy projections are those based on ample experience; what is past is prologue; what happened before will likely happen again, and about as often unless circumstances have changed greatly. That is why you went around collecting statistics before you started interviewing.

Talking about AFE is talking about probabilities, the likelihood that a particular mishap is going to materialize in the next year. Those estimates based on actual experience will be statistically reliable if the mishap occurs often enough and the universe is large enough. This is the kind of firm information that makes us feel comfortable and sure of ourselves. But many of your projections will have to be made without benefit of experience and will have no statistical reliability. However, they will not be off-the-wall estimates, they will be estimates based on the best information available, the informed opinion of experts who know their field as well as the operations under study. Because the AFE is often not a cut-and-dried projection, this entry should always be justified, explained on the back of your worksheet. More about explanations later, right now probabilities that can range from absolute certainty to mere possibility are being talked about. Risk assessment is not satisfied with mere possibility, after all, it's 100 percent possible that your building will burn down sometime in the next 12 months, but it is the 1 percent probability that interests us. All frequency estimates, the AFE you wind up putting in this little box, represent your belief as to how likely it is that this particular mishap will occur. It is your best guess after interviewing your experts. You would be surprised how often people put a figure in this box and then go on to explain why it is not realistic. To make it handier and easier for you to convert your probability estimates to the nice, neat, annual frequencies so convenient to work with, the conversion chart has been simplified and put it on the left margin of your worksheet.

The days, weeks, months, and years have been left off because they are whole numbers and it is easy to figure out that something happening an average of once a week happens 52 times a year and that 52 would be the AFE. Besides, it gets us out of the bind of saying once-a-day means 365 times a year when your operations may run only 260 days a year. Conversions are most helpful when you are trying to apportion the risk of something that happens less often than once a year. For example, something that might happen only once every 2 years is very easily thought of as the fraction 1/2, meaning 1 time in 2 years. Once every 15 years is the obvious fraction 1/15. Once every 400 years would be 1/400 or 1 chance in 400 that something is going to happen in the next year. But decimals are easier for most of us to work with, so these fractions have been taken and given their equivalent decimal values; e.g., 1/75 = .013 to indicate that something that might happen once every 75 years equals an AFE of .013.

The example shown poses no AFE problem because the power outages are happening so frequently it is not necessary to guess, and so do not even worry about fractions. A similar example might be lost tapes. Lost for good, or lost long enough that they were as good as lost for good. Anyway, you could not find them when you needed them and had to copy your backups from source documents. In short, not being able to put your hands on the tapes when you needed them costs you something; either money, delay, or possible unauthorized disclosure - you get the idea. Does this happen a lot? Are there any records? Is there anybody around who would have a better fix on this particular risk than the person you are interviewing? If you find that it happens every couple of months, you have estimated frequency of occurrence for losing or misplacing tapes. If something happens this often maybe somebody will decide to tighten the controls. Who knows? What you and your expert recommend will also depend on impact and the cost of better controls.

You will find it impossible to develop a meaningful AFE for impacts expressed as a range; e.g., 1 to 10,000 records improperly disclosed. What are you going to multiply by, 1 or 10,000? So if you have a problem here, the problem is not here, it is one block up. Block E should be averaged out, if it can be sensibly averaged, or it should be split up into different risks and those that are significant handled one at a time. For example, disclosures of 400 records should be handled on one worksheet and disclosures of 5,000 on another.

So far things your organization has experienced time and time again have been considered, no problems forecasting here. But what if something happened only once or twice in living memory?

You do two things:

(1) You and your expert put your heads together and come up with an estimate that seems realistic and explain your rationale on the back of the worksheet. Briefly, if possible, but this a good time to remind yourselves that money will be spent, or risks accepted, based on your estimates and how well you support them. Management is going to want to know more than just figures before making any decisions to budget, or not budget, for specific safeguards. They know you are estimating and do not want you to panic over pennies. On the other hand, they are going to expect reasoned thought; "wild guess" will fail to amuse. If you are going by gut feeling, yours or your operational experts, something is making you choose once every 10 years (.10) over once every 50 years (.020) so let your management and reviewers know what is going through your mind. The risk assessment worksheet is designed to stand-alone; nobody should have to call you up for an explanation of your probability estimates. Part of your explanation might be that your expert has been an application programmer for 15 years, with three major companies, and has seen this mishap occur only once, and that was without all the safeguards in place in your organization. Another might be that you contacted several outside authorities (name them) whose inputs averaged out to the AFE used. Your reasons should be something a person can agree or disagree with. Not just, "This is my considered opinion," folks have to know why it is your considered opinion.

(2) Second is a personal message to your CCMO and HCFA Project Officer, right there in the Comments block if you want to contribute to the risk assessment data pool. Show how often the event actually did happen, and over how long a period. For example, if your organization has been a Medicare contractor for 12 years and suffered one power failure in that time, show, "Power failure caused $13,000 damage and 5-day delay once in 12 years." You may be ask more particulars so to better relate your experience with the experience of other business partners to provide guidance to still other partners with no experience at all. Adequately defined, this pooled information should save a lot of head scratching down the line. Everybody likes firm figures, and where can figures be firmer than from our business partners in the Health Care Finance field?

It confuses humans to figure risks in terms of long periods of time. Like thinking your building is not going to burn down for another 300 years. What you are really after is odds. What are the odds your building is going to burn to the ground in the next year? If this is June 9, 2000, what are the chances it will go up in smoke by June 8, 2001? One chance in 300? Put another way, if there are 300 buildings like yours, one of them, maybe yours, is going to burn up in the next 12 months. Your building manager or your fire marshal or your fire department, or your insurance company, may be able to give you a good idea of how likely it is that a building in your class will be destroyed, whether they express the risk in years or odds or percentages.

Insurance premiums are often a percentage of your building's assessed valuation. A five percent premium means that in 20 years you have paid for the building. Of course, they are in business to make a profit. Arbitrarily, you can triple that 20 years for a 60 year frequency estimate. A little crude, but every organization's fire insurance is based on considerable assessment of many factors, so why not piggyback? Maybe your fire chief or insurance man can suggest a better way to relate premium to probability.

If your building is in a floodplain, your county should be able to help you with your frequency estimate. They might be able to tell you that you are in a 100-year floodplain, meaning you are close to a creek or stream or river that could flood you out, and the probability of flooding once during any given year is considered to be 1 percent, an AFE .010.

Sometimes the only way to estimate frequency of occurrence is by talking to experts who are knowledgeable enough in their field to suggest something reasonable, based possibly on what they know from talking to others, attending conferences, symposiums, etc. For example, fraud is one of those things few organizations admit being victim to, at least in print, so word-of-mouth is often the only way to get a feel for how much of a problem this is generally. At professional gatherings, you or your operational expert may exchange business cards with your respective counterparts; such contacts are often thought to be career-opportunity enhancing. Risk assessment gives you the perfect excuse to keep in touch. Besides, everybody likes to give advice; it is getting somebody to take it, that is the problem. In risk assessment, mere opinion is not worth much but informed opinion is.

Maybe this is the place to emphasize just how broad a conscientious frequency projection can be. It is entirely legitimate to ask your expert these questions:

- Does it happen 100 times day?
- Ten times a day?
- Every Day?
- Every 10 days?
- Every 100 days?
- Every 3 years?
- Every 30 years?
- Every 300 years?

It is all right to be no more specific than this. If this is as specific as you can get. It is the old orders-of magnitude method.

Here are some questions that might help you develop AFEs:

- Are statistics available on this risk relative to this asset and operation?
- Have any safeguards been installed recently that might affect existing statistics?
- Do you have any idea how much of a problem this is in other organizations?

- Is there anyone else who might have a good idea of the probability?
- Can you phone any of your outside contacts for an opinion?
- For the rationale, what are some of the things that make you think the risk will happen as often as estimated (or as seldom)?

G. Annual Impact Estimate (AIE)

Here you enter what you get by multiplying your NIE by your AFE. The answer will be dollar-loss-per-year, or the number-of-records-per-year that were disclosed without authorization, or the number-of-days-per-year that Medicare operations were delayed. Would you believe you've just done a risk analysis? The rest of your worksheet is for suggesting safeguards and costing out their effectiveness. In the example, the $37,500, 2-day impact doubled, making it twice as important to do something than the impact per se, would indicate.

Dwell on this a moment because some people tend to think of impact as risk. It is not. A million dollar mishap sounds impressive but gets cut down to size when diluted by time: $1,000,000 X .022 = $2,200. You would not want to spend outrageously to safeguard against a large loss that has only one chance in 400 of happening in the next 12 months. Other people, on the other hand, point out that your number could come up tomorrow no matter what the odds, and if it does, you could be out of business because the loss is so staggering. True. Which is why your management should be told NIE plus AFE, not just AIE. All things seldom being equal, the boss may decide to treat identical AIEs differently, weighting in favor of the high impact loss.

H. Scale of ANNUAL Impact Priorities

Do not fall in love with the notion that risks can be graded small, Medium, or LARGE (The block H on the Medicare Risk Analysis worksheet). These designations are based on the quantifications in Block G and are not supposed to be independent qualitative estimates as in fuzzy metrics. The only reason for including a scale of annual impact priorities is to make it possible for you to prioritize different kinds of risk when you start summarizing your worksheet findings for management's action. Large risks first, medium second, small bringing up the rear. Large disclosures would come ahead of medium dollar loss, etc.

The example illustrates the fact that some mishaps have more than one kind of impact. In fact, dollar loss is often associated with operational delays, so consider both when establishing priorities. Of course, the reason for expressing loss in things other than dollars is to avoid either ignoring mishaps not measurable in money or trying to force non-monetary impacts such as disclosure into dollar values, and you know how hard it is to find dollar values these days.

One vast improvement suggested by contractors is including the actual amounts right in this block on the worksheet. It is certainly handier and serves to emphasize that small, medium, and large have absolute values and do not "mean what you want them to". So now instead of circling S, M, or L as appropriate, circle the given value as appropriate. You may be using the "records disclosed" impact to include sensitive listings of things like an array of physicians' annual Medicare payments. If you want, you can make your own category for impacts other than the ones listed, but prioritizing is not that big a deal, so the space designated "OTHER" does not appear.

If there was room, "DAYS' DELAY" would have been changed to "DAYS' DELAY IN MEDICARE OPERATIONS FOR THE ENTIRE BUILDING OR COMPONENT UNDER CONSIDERATION", because that is what is meant. If you start figuring “days delay” per claim, you soon run off the other end of the calendar which is limited to 365 days, give or take a leap year. "Delay" impacts were thought up to handle disaster-type impacts that shut down whole departments, causing interruption of mission, hence substantial inconvenience to Medicare beneficiaries. You are used to dealing with backlog statistics in terms of individual claims delayed, but risk assessment deals with bigger delays. So, if you estimate that an error might delay a significant number of claims, you can stay in the big-deal scale by figuring what the daily claims output is for that department and dividing this figure into the number of claims delayed, then multiplying by the number of days they would be delayed. Complicated? Not at all. Output averaging say, 1,000 claims per day would be divided into the 100 claims delayed (100 divided by 1,000 = .1) and the result multiplied by the average delay of 30 days (.1 X 30) which gives a nice medium delay of 3 days; something you can stack up against medium dollar losses and disclosures. Of course, this is the kind of fancy figuring that should be put on the back of the worksheet and explained.

"Delays" means consecutive days delay which automatically eliminates delays of a single day. Even 1 day's delay 10 times a year would not be in the running at all because it is not consecutive. But 2 consecutive days 10 times a year would give you 20 days a year, which is large though they are not all consecutive, which is why "consecutive" is not used in this block. It's a little weird, but you can still use the chart as a guide; once prioritized, the risk can be re-evaluated by management. Management is going to give special weight to high-impact delays, meaning worry more about a 30-day delay once every 10 years than a 15-day delay once every 5 years even though they both average out to 3 days a year, especially where computers are involved. But don't get the idea that prioritization doesn't work for operational delays, because it does. A delay can be figured both in dollars and in mission delay; so a very long delay, say 60 days, that got dissipated to insignificance because it should not happen but once every 75 years. This delay might result in such a big money loss that the priority for the annualized dollar impact would still remain large and deserving of high-dollar hand wringing.

The best is saved till last. ANNUAL is capitalized to emphasize that impact is not what matters but what impact works out to per year. The principle of insurance is to spread the risk, and risk assessment spreads the risk over time.

I. Additional Safeguards to be Considered

First you have to decide whether or not extra safeguards might be worthwhile. Some will be so cheap and obvious and easy to do that you do them and make a note on the back of the worksheet so you can give yourself a pat on the back when reporting to management.

But say you do feel that the AIE for a particular risk warrants spending some money for additional safeguards. Provided is a list of various kinds of safeguards to suggest different possibilities to you, and to steer you away from all-purpose measures like "orientation" and "planning for contingencies" that are required anyway in your organization's security program.

Please use the code numbers when identifying the safeguards, but be a little more specific in your description than, for example, "Restricted Access" which could mean guards or locks or bars-on-the-windows. The very best risk analyses are not stingy with explanations, you should be able to look at the worksheets and get a clear picture of what safeguards are actually being suggested for management consideration.

There is space for three recommendations. A recommendation is any safeguard entered in Block I, columns #1, #2, or #3, that you do not line out before you sign the worksheet and turn it over to your management. Preserve the tentative recommendations that did not turn out so hot. What had struck you as a pretty good idea at the time will probably strike management the same way. They will want to know why you are not recommending some apparently effective safeguard and it would be nice if the worksheet showed the safeguard, the calculations through Block U (which should show why that safeguard was a dud) and the "X" or line through that column plainly indicating that you are not recommending it after all. If, for some reason, your figures are not self-evident, you can explain your decision on the back of the worksheet. It may be that the "deleted" safeguard was not all that bad, but several others seemed better and cheaper upon reflection.

Originally add-on safeguards; columns #2 and #3 were intended to build upon safeguard #1, just as safeguard #1 built upon the present safeguards listed in block D. All of which is still possible. But it turns out that proposing alternative safeguards helps managers and reviewers figure out the best way to go. It makes them feel good to have options so they can pick and choose and study feasibility to their hearts content. After all, some dynamite safeguard simply might not be affordable right now, so management would appreciate having a choice that is less costly even if less effective.

So without complicating things too much you can go both ways. You are given the and/or option in Block I, and a way to signal which way your are going: check the upper box in column #2 if you are proposing this safeguard in addition to (with) the safeguard proposed in column #1; check the lower box if you want safeguard #2 considered all by itself instead of #1. Same principle is followed for column #3. This way, 7 months from now everybody knows what you had in mind when you completed the worksheet and they won't have to call you up with questions you can't remember the answers to.

There is one thing you will want to check if you have not done so already, your core requirements (safeguards). It might be frustrating to recommend a particular safeguard and still find yourself out of compliance. Let's expand on this thought, because people have a hard time relating risk assessment to the rest of the program, which consists of additional administrative measures plus the core security requirements. You always do risk assessment with one eye on the requirements because risk assessment indicates where you should exceed specific requirements or seek waiver from those requirements that do not seem cost-justified. (Administrative measures like risk assessment itself, contingency planning, screening personnel, and cooperating in external reviews are never subject to waiver, constituting the very fabric of systems security.) In short, it is a good idea to know where you are out of compliance with requirements so you can be sure to include these areas in your every-3-year risk assessment. Did you realize that waivers expire every 3 years? So if you work things right, you can work your waiver re-justifications right in with your triennial risk assessment.

The example shown proposes two safeguards, the second supplementing the first. This illustrates the principle of layering; different safeguards often enhance one another like 1 + 1 = 7, in effectiveness. Another classic example is reducing the potential for unauthorized disclosure and fraud by putting locks on terminals <u>and</u> installing a functioning password system; together they are about 10 times as effective in protecting your data base as either would be by itself. (1 + 1 = 10.)

The multiple-effect worksheet has been eliminated. This was because the risk assessment worksheet itself has been made so complete that the assessment can be carried all the way through to the computation of net savings. Now, multiple-effecting, which sounds complicated, can be done so simply that you can just add up a few things on a blank piece of paper and staple the paper to the worksheets involved. More about this later.

Here are some questions that might get your expert thinking along constructive lines:

- What would be the first thing you would suggest to reduce the likelihood that this risk would happen?
- What would be the first thing you would suggest to reduce the consequences if the risk should happen?
- Are there additional, complementary safeguards that could reduce probability or impact further?
- Are there other ways to reduce impact or probability?
- Are there cheaper ways to go?
- Are there any safeguards that might also reduce the risk for another asset or operation? (If so, flag the worksheet for attachment to other worksheets proposing the same safeguards.)
- Are there any safeguards that might also reduce a different risk? If so, flag them.

J. NIE Revised to Reflect Additional Safeguards

This block title means that the impact originally estimated is being estimated anew to show the effect of the proposed safeguard.

At one time, any proposed safeguard was believed to reduce either impact or probability but not both. It is now believed that most safeguards do either, but some do both. For example, a safeguard designed to detect fraud earlier than is presently possible would certainly reduce impact but it might also reduce probability because employees tend <u>not</u> to tamper with systems known to be booby-trapped. At any rate, it is true that you would not recommend any safeguard if it is not going to do something nice for you, and your job in block J is to figure out whether it is going to reduce your net impact, and if so, how much. You do not enter the amount of the reduction. You <u>do</u> enter the reduced net-impact-estimate. For instance, in the example it was figured that a bank of batteries is going to go a long way to reduce the net impact of the power outages. Then ask the question, "What if we already had racks of batteries in the basement to keep the computer facilities humming along long enough to degrade ourselves with grace and aplomb?" Answer: $25,000 instead of $37,500. Had this been the kind of safeguard that would reduce probability but not impact, we would have gone with our original estimate, $37,500.

You probably will want to go through all your calculations for the battery safeguard, then do a number on the backup generator. But here you are covering each block to a conclusion, so let's do for safeguard #2 what you just did for safeguard #1. The important thing to keep in mind is whether #2 should be considered with #1 or instead of #1. If "with," you start off with the NIE revised in Block J, column #1, right next door. If "instead of," you start off with the NIE way up in Block E, just like you did with safeguard #1.

Don't forget to carry through your calculations for all impacts. The example shows that batteries do not change the delay impact, so still show 2 days as was done in Block E. But batteries plus the generator solve all our problems, no more dollar loss, no more delay, a happy projection reflected in J-2 (that's Block J, column #2.)

Estimating is guessing, let's face it. But remember two things:

- First, you've got to have good reasoning behind your estimates, something you could defend to management;
- Second, you are not engaged in a precise accounting-type function and it might help limber up your mental muscles if you think in percentages scaled no finer than 10 percent, 20 percent, 30 percent, etc., through 100 percent.

To demonstrate: if you figured that an additional safeguard might reduce NIE by about 30 percent, you would simply enter 70 percent of the previous NIE.

Questions for your expert:

- How much might the additional safeguard #1 reduce the cost to recover from the risk?
- Does it also reduce delays or disclosures?
- Is there a breakdown of the original NIE that might suggest which items would be affected by the additional safeguard?
- Is safeguard #2 (or #3) a supplement or a substitute? (Calculate accordingly.)

K. AFE Revised To Reflect Additional Safeguards

For each proposed safeguard, figure how much you have reduced the likelihood the mishap will occur. If you have, you and your expert might be more comfortable thinking in percentages or in scales of one-to-ten. Keying everything, of course, to the applicable annual frequency estimate (AFE). The applicable AFE for safeguard #1 is always the AFE shown in block F, so your AFE for safeguard #1 is a percentage of the present AFE in Block F. (From 0 percent to 100 percent.)

If safeguard #2 is to be evaluated all by itself, meaning "instead of #1" and not "with #1," figure how much #2 reduces the present AFE in Block F, just as you did for #1.

But, of course, if you are recommending the second safeguard to supplement the first, you show how much #2 reduces the AFE shown in K-1. You are trying to tell management, "Look, if you do #1, this is what you get, and if you also do #2, here's what extra you get." This way management will know the cumulative effect of each of the additional safeguards that you want them to consider buying. It is as if you are pretending that the first safeguard had already been installed, and now you want to see what more could be accomplished with a second safeguard.

Here is a way to phrase your questions so that your expert will know what it is you want:

- Do you think that this safeguard might reduce the probability that this risk will materialize, might make the mishap less likely to happen? If not, just repeat the previous AFE. (If the answer is yes, but it is not obvious how the safeguard could reduce probability, ask him to think up some examples.)
- How much do you think safeguard #1 might reduce the odds that this mishap will occur? (Look at the present AFE and pick a new AFE from the chart on your worksheet.)

How about alternative safeguards: how might they reduce the present AFE? (Pick a winner from the chart.)

What about additional safeguards, the ones that may further reduce AFE: how much do you think they might reduce the new AFE we just came up with for the previous safeguard? (If no reduction, enter the AFE for the previous safeguard; if there is a reduction, pick a lower frequency from the chart.)

L. AIE Revised To Reflect Additional Safeguards

For each proposed safeguard, multiply new impacts by new frequencies to get new net AIEs (noted in L-1 and L-2). In the example, safeguard #1 does not affect the AFE so we put in the same AFE that was used to show the probability of the present risk. Safeguard #2 on the other hand, does change AFE, eliminates it, as a matter of fact, so do not merely carry forward the AFE in K-1 but reduce it to zero. (Because this is an add-on safeguard, something to be considered in addition to safeguard #1, looked at the K-1 AFE instead of the AFE in Block F; in this case they happen to be the same. If #2 were offered as an alternative to #1, then look at the present AFE in Block F just as was done for #1.)

M. Annual Cost of Each Additional Safeguard

You may have to make some phone calls to price out some of the proposed safeguards. And don't get hung up on the idea that you're proposing safeguards that might turn out not to be cost-effective. You can un-propose them by drawing a line through them. (But don't obliterate them altogether; give management the benefit of your assessment.) In the example, it would have been easy to forget about maintenance cost of the batteries and generator; there is tendency to think of annual expenditures more directly, like so-much-salary-and-fringe for an extra reviewer to reduce errors. But we didn't forget and were able to find out what it costs to keep up a bank of batteries and a generator ready to cut in when power cuts out.

A question for your expert:

- What might each safeguard cost to maintain each year in terms of supplies, personnel, slow-down of operations, new hires, and increased costs of operations elsewhere?

N. One-Time-Cost (OTC) of Each Additional Safeguard

You or your expert might recommend a safeguard that might represent a bit of an expenditure, but one that might pay off in the long run. In the example, the vendors came out and gave us estimates that seemed reasonable for a bank of batteries and a generator that would do the job. Anything that seems out of line could be checked with other business partners who already have such protection. Or get somebody else out to give you a bid. Remember that the worksheet is for Medicare's fair share of any safeguards. You won't want to lose track of the total amount, so you can put that on the back of the worksheet; this way, management will have no ugly surprises when they learn that that $50,000 safeguard actually costs $100,000. It could have been done the other way, asked for the total cost before sharing, but this way is clearer, everything on the front of the worksheet applies to Medicare.

Here's a question that might help your expert think of start-up costs for some of the safeguards you've jointly proposed:

- What nonrecurring costs might result from each safeguard for such things as equipment, labor, materials, moving things around, renovation, construction, alarms, devices, costs of installing systems, etc.

O. AIE From Block G

You're almost finished. This block merely repositions a figure developed earlier, puts it here where it is convenient to work with.

So far safeguards have been addressed using columns #1, #2, and #3. When you're working with column #1 (for safeguard #1, of course) it's simple to bring down the data you need, just go to the block specified in this case Block G. You do the same for column #2 if that safeguard is being suggested as an alternative to #1.

But you go to a different "register" if your second safeguard is to be considered in conjunction with safeguard #1. Because #2 depends on #1 to achieve whatever additional benefit is to be realized. You are building on safeguard #1. The note "* from L-1 if with" means, of course, that you bring down the figure in Block L column #1 and enter it in Block O column #2; you do this whenever safeguard #2 is checked "with #1" up there in Block I. (If the little box in front of "instead of #1" had been checked (or X'd), you would use the AIE from Block G because that means safeguard #2 is to be considered independently of #1 as an alternative, an "either/or-but-not-both" choice for management, requiring that the effect of each safeguard be costed out separately.)

When dealing with safeguard #3, the same principle applies. If #3 is alternative to #1 and #2, use the AIE from Block G. But if you're layering your safeguards and #3 must be considered "with #1 and #2," then you get your figure from Block L column #2 which shows what the annual impact estimate would be if safeguards #1 and #2 were already in place and working.

We did not give you the option of considering #3 with #1, but not #2 or vice versa, because there's a limit as to what can be effectively done.

The example brings down that $75,000 from Block G for safeguard #1, but goes to L1 for the revised $50,000 AIE which lets you consider #2 as if #1 were already installed, which is what you signified you would be doing when you checked "with #1" in Block I column #2.

P. AIE From Block L-1**

The double asterisk here is to alert you to the fact that the Block L column 1 figure is used across the board only when the additional safeguards are not linked together and can and should and must be treated separately. When the second safeguard is linked to the first, and the third is linked to the other two, then the cumulative effect is calculated if management is to be properly guided in its decision-making process. The little notes in Block P, columns #2 and #3, tell you where to get the figures you need when I-2 and I-3 are checked "with."

In the example, $50,000 and the 4-day delay was brought down from Block L column #1 for obvious reasons, we wanted to calculate savings, or the reduction of disclosure/delay impact attributable to the bank of batteries hereinafter referred to as safeguard #1.

Not so obviously, in column # 2 the figures in L-2 were used, because we wanted to show the additional impact-reduction figures reflecting the situation as it would be if safeguards #1 and #2 were already in and working. (To find out what additional savings the generator will generate, we'll soon be subtracting this from the L-l AIE now shown in O-2.)

Q. Gross Annual Savings

Here you get figures showing what your proposed safeguards will do for you. "Savings" implies dollars but actually includes things like days saved, and disclosures saved. Because you had previously converted everything to a yearly basis, your answers come out in yearly savings.

Each column shows, of course, the savings attributable to each safeguard (O# minus P# = Q#). It's nice to keep in mind that the savings calculated for layered safeguards are predicated on the premise, or based on the assumption, that the previous safeguard(s) (e.g., #1 or #1 and #2) will be in effect. So once you have signaled that safeguards 2 or 3 must be considered "with" the other(s) you can't look at the savings and say, "This is what we might save," without adding, "on the assumption that the safeguards listed to the immediate left are also implemented." On the other hand you or management can lop off safeguards to the right and still have valid estimates for the ones remaining. Meaning #2 depends on #1 but #1 does not depend on #2.

In the example, gross savings of $25,000 could result from installing batteries, but no days' delay are saved, meaning you are not helping things "delaywise" even though you are "dollarwise." But given the installation of batteries, your generator is going to save Medicare an extra $50,000 and 4 days' delay. Without the generator, the batteries are still going to save you $25,000; without the batteries, the generator is going to save you ????. You don't know because that is not how you figured things; you recommended a package deal. If you suspected that management might go for generators and not batteries, you might have wanted to switch them around; as safeguard #1, the generator would generate savings independent of safeguard #2, just as the batteries did when they were #1. Lastly you could have checked the instead of #1&2 option in I-3 and costed out a standalone generator option.

R. Annual Cost From Block M

This is just a simple, direct transfer of amounts from M. What is in M-1 goes into R-1; what is in M-2 goes into R-2 and M-3 into R-3.

See that in the example the $1,000 shown in M-1 turned up in R-1, and that R-2 reflects the $3,000 up in M-2.

S. Net Annual Savings Without OTC

Subtract R from Q and you get what the caption promises. In the example, $24,000 for #1 (batteries) and an additional $47,000 for #2 (generator). Plus that 4-day delay, which really is minus the 4-day delay that the generator eliminates?

T. One-Fifth of any OTC Shown in Block N

This is a way to handle one time costs (like the big initial outlays for the batteries and generator) without having to project savings over the arbitrary payback period. You simply do it the other way around; you keep your 1-year savings but fracture your OTC. Instead of showing the full OTC in relation to 5-years' savings, you show 1/5 of the OTC in relation to 1 year's savings. It is the same difference and your answer is still annualized.

Doing it with the example, you come up with $8,000, which is 1/5 of the $40,000 worth of batteries shown in N-1; and we get $20,000 in T-2, which is a mere 1/5 of the total cost to Medicare of that brand new generator proposed in N-2.

U. Net Annual Savings

At last the bottom line. If you have been both conscientious and convincing, this is what management will rely on for those "informed decisions". Just subtract T from S and you have it, but don't forget to bring along those non-monetary savings, meaning disclosures, and delays and anything else you can think of; these things might just tip the scale in favor of safeguards that are not strictly cost-justified.

The example tells management that they can save a projected $16,000 by installing the backup batteries you are recommending; and another $27,000 by springing for the generator, not to mention (or rather to mention) saving 4 days' downtime every year. Your computations have been conscientious, but have your comments been convincing? Having gone this far, you do not want management to discount your entire risk assessment. For more details, see V below.

V. Use Other Side for Explanations, Comments, Rationales, Sources, Contacts, NIE Calculations, Etc. KEY REMARKS TO APPROPRIATE BLOCKS

Most risk analyses tend to be too talky. Words without facts and figures. The worksheet takes care of this problem. But, let's not do the opposite; let's not eliminate legitimate explanations or the calculations that just may give credence to those facts and figures so laboriously developed on the front of the worksheet. This is particularly true of those NIE calculations that show hourly rates, insurance coverage, etc., to show that you did really and truly consider everything when coming up with your Final Figure. And most especially, justify those probability estimates, showing how they were developed and who was consulted, even negative findings (I asked the Computer Institute but they wouldn't hazard a guess) show what bases you touched.

The highest compliment you can receive is to have management go with your recommendations without having to call you in to explain your assessment. You stand behind it, but your risk assessment worksheet should be able to stand on its own.

W. Prepared By and Date

This block validates your risk assessment. Without it, the worksheet is mere speculation by person or persons unknown at some unspecified time. Signing and dating your worksheet certifies that it was done by a responsible and competent analyst and represents the best estimates deliverable at a particular point in time and space. Sign and date the worksheets.

5. Multiple Effecting (Rev. 1 -- 01-26-01)

Really, one of the biggest problems in risk assessment is sorting things out, avoiding situations with endless ramifications. Indeed, this is the most compelling reason for excluding all-purpose administrative type safeguards from risk assessment, the effects of something as all encompassing as contingency planning is so far-reaching that you would never get done costing out the effects.

Even a specific safeguard, however, may often reduce several risks simultaneously; and even when the safeguard is specific to a single risk, the effects may spread throughout the organization, far beyond the component under study.

So what do you do? Any time you recommend a safeguard that will have these multiple effects, make up new worksheets for these other risks or components (or both) and complete each worksheet independently. (This assumes that you have tried to handle risks at the highest practical level in the first place, like analyzing fire-and-smoke damage at the whole-building level instead of one component at a time.) Then when you get all through doing individual worksheets that have a common safeguard, you put them in a pile for multiple effecting.

Another situation is when you get all through with your organization's risk assessment; you then sort through all your worksheets to see if any of the same identical safeguards have been recommended more than once. Put these into piles (one pile per safeguard) and get ready to multiple effect.

A third situation and this is going to save you having to do your waiver requests twice, the third and most usual situation is when you are seeking relief from compliance with a required safeguard. Here it is the safeguard you start off with as you complete each worksheet; trying to figure out whether or not the required safeguard is for you, may take several worksheets because the safeguard may have several effects. You complete a worksheet from start to finish for each risk the safeguard might address, then figure out the multiple effect for each of these safeguards that have more than one worksheet. (You may surprise yourself; the safeguard may turn out to be cost-effective after all!)

"Multiple effecting", it sounds impressive, but is actually so simple a process that there is no worksheet. All it takes is a pen, a blank sheet of paper, and a stapler. Your worksheet computations are all complete and valid except for those situations where the same safeguard is recommended more than once. In that case you have a distortion. You are not suggesting that management buy the same safeguard six or seven times (as your six or seven separate worksheets might imply.) You are recommending that the management buy it only once. Now, what you want to do is to tell him all the wonderful things this safeguard is going to do for Medicare. So you take this blank sheet of paper and add up all the Gross Annual Savings attributable to this safeguard (from Block Q of each worksheet) and deduct the single Annual Cost of the safeguard (Block M). (Do not add up the cost from each sheet!) Your answer represents the Net Annual Savings without OTC for all the risks this one safeguard reduces. Next, you deduct 1/5 of any OTC for the safeguard (Block T) and you have your multiple effect for this safeguard, which is <u>all</u> the dollars, delays, and disclosures it saves you.

Do not forget to include those worksheets where the safeguard was <u>not</u> cost-effective for the particular application. That is one of the beauties of multiple effecting, justifying a safeguard that might be considered a dud taken risk-by-risk or component-by-component when that does not tell the whole story.

You may have two or three other safeguards suggested on one of the worksheets you are going to be setting aside for multiple effecting. Reproduce that worksheet for your multiple effect pile, and be sure to make a note on the original stating what you did and why.

One final word: Staple all those worksheets to the sheet of paper on which you have calculated the multiple effect. To separate them from the mother-sheet confuses everything because taken singly they are not part of the big picture, they are distortions. (Flagging or annotating each such worksheet helps, but grouping and stapling is essential and a kindness to those who come after.)

6. Summarizing for Management Action (Rev. 1 -- 01-26-01)

The worksheet tells the whole story from Net Impact Estimate to NET ANNUAL SAVINGS! But you're still going to have to do a management summary. Although there are many benefits to be gained from conducting a conscientious and comprehensive risk assessment, the main goals are to tell management where Medicare assets and operations are most at risk and to recommend what should be done.

Systems Security Must Compete With Other Budget Items "For Its Share of Available Funds". How much money management earmarks for fire extinguishers and security software and uninterruptible power and audit routines and water alarms and procedural changes and shredders and training and backup tapes is going to depend on the summary you write based on all your work and all your worksheets. The decisions are not yours to make but the <u>inputs</u> are yours. Your narrative summary has to be complete enough all by itself for management to make decisions and convincing enough to inspire action. Facts, figures, judgements, rationales laid right on the table. Not just defensible, never merely informational, but clear and compelling.

MEDICARE RISK ASSESSMENT CHECKLIST

Building or Component Prepared By Date

Circle Code # if Condition Exists in Your Building or Component.

101 Building is old
102 Building has non-HCFA tenants
103 Building is in a high crime neighborhood
104 Building is in a tornado area or earthquake zone
105 Building is far from a fire station
106 Component has large electrical equipment/machinery
107 Component has highly burnable supplies, equipment, furniture, etc.
108 Component has false floors
109 Component is on the ground floor or lower and your building is in flood plain
110 Component is located on the top floor
111 Heavy equipment on floor above (or roof)
112 Equipment is old
113 Equipment requires air conditioning/climate control
114 Component has a sprinkler system or bad plumbing
115 Component is undergoing alterations/repairs (or will be shortly)
116 There is employee dissatisfaction or labor-management
117 Data produced, used, or stored has value to others
118 Data could be used to defeat safeguards or exploit vulnerabilities
119 Data could be used to distort test results or gain unfair competitive advantage
120 Data might be material in legal actions
121 Data might embarrass the Medicare program or recipients if in wrong hands
122 Some employees are new and/or unaware of procedures
123 Some employees work under very tight schedules
124 Some employees eat, drink, or smoke in the component
125 Equipment/supplies are valuable, portable, and marketable
126 Equipment/supplies would be personally useful to employees or others
127 Strangers/customers/visitors are not unusual in the component
128 Component is near an exit opening on to street or parking lot
129 Equipment could be used on site to conduct non-HCFA business/hobbies
130 Operations involve disbursing/receiving payments
131 Emergency payments are common
132 Actual practices differ from official procedures

Attachment 1

MEDICARE RISK ASSESSMENT MATRIX

BUILDING OR COMPONENT:___________________________________

	ALL MEDICARE ASSETS								
CHECK BOX ONLY IF YOU FEEL		EDP Systems and Data							
THAT THE RISK MIGHT			Non-EDP Data						
AVERAGE OUT TO AT LEAST:				Computer Facilities					
$1000 Net Lost per Year, or 2 Days					Mini-Micro Computer Facilities				
Delay Per Year, Or 10 Records						Remote Workstations and Links			
Improperly Disclosed Per Year							Ancillary Facilities		
								Other Medicare Assets	
	200	210	220	230	240	250	260	270	_____________________ ______ Prepared by Date
									PEOPLE TO BE CONTACTED
410 ALL DISASTER									
411 Fire and smoke									
412 Storm Damage									
413 Earthquake									
414 Explosions									
415 Civil Disorder									
416 Flood									
417 Other Disaster(specify)									
420 ALL DISRUPTION									
421 Water Damage Other than Flood									
422 Vandalism/Sabotage									
423 Strikes and Job Actions									
424 Power Failure/Malfunction									
425 Air Conditioning Failure									
426 Heating Failure									
427 Machine Failure/Malfunction									
428 Other Disruptions(specify)									
430 ALL AUTHORIZED DISCLOSURE									
440 ALL ERROR									
441 Errors/Omissions									
442 Accidents									
443 Erasures									
444 Losing/Misplacing Assets									
445 Other Errors(specify)									
450 ALL THEFT									
451 Theft of Assets									
452 Theft of Services									
453 Other Theft(specify)									
460 ALL FRAUD									
461 Fraudulently Blocking Transactions									
462 Entering Bogus Transactions									
463 Altering Systems Programs									
465 Altering Records/Data Base									
466 Other Fraud(specify)									

Attachment 2

MEDICARE RISK ASSESSMENT WORKSHEET

1/2 =	.5
1/3 =	.33
1/4 =	.25
1/5 =	.20
1/6 =	.17
1/7 =	.14
1/8 =	.12
1/9 =	.11
1/10 =	.10
1/15 =	.067
1/20 =	.050
1/25 =	.040
1/30 =	.033
1/35 =	.029
1/40 =	.025
1/45 =	.022
1/50 =	.020
1/60 =	.017
1/75 =	.013
1/100 =	.001
1/200 =	.005
1/300 =	.003
1/400 =	.002

A **Code**	Name of Component	**B** **Code**	Describe Risks
C **Code**	Describe Medicare Assets and Give Locations	**D** **Code**	Describe Present Safeguard

E **Net Impact Estimate (NIE)**	$
F Annual Frequency Estimate (AFE)	X
G Annual Impact Estimate (AIE)	-

H **Scale of ANNUAL Impact Priorities**

	Small	**Medium**	**Large**
Dollar Loss	$1,000 to $5,999	$6,000 to $25,999	$26,000 Plus
# Records Disclosed	10 to 25	26 to 50	31 plus
Days Delay	2	3 to 6	7 plus |

I Additional Safeguards to be considered, if any. (Cross out, but do Not Obliterate, Those safeguards that you would not now recommend to your management)	**# 1** **#1**	**# 2** □ with # 1 □ instead of # 1 **#2**	**# 3** □ with # 1 & 2 □ instead of # 1 & 2 **#3**
J NIE Revised to reflect Additional safeguards	**$**	**$**	**$**
K AFE Revised to Reflect additional safeguards	**X**	**X**	**X**
L AIE Revised to Reflect additional safeguards	**=$**	**=$**	**=$**
M Annual cost of each additional safeguard	**$**	**$**	**$**
N One-Time cost (OTE) of each additional safeguard	**$**	**$**	**$**
O AIE from block G*	**$**	**$** ***** from L-1 if with	**$** ***** from L-2 if with
P AIE from block L-1 **	**-$**	**-$** ****** from L-2 if with	**-$** ******from L-3 if with
Q Gross Annual Savings	**=$**	**=$**	**=$**
R Annual Savings	**-$**	**-$**	**-$**
S Net Annual Savings without OTC	**=$**	**=$**	**=$**
T One-Fifth of any OTC shown in Block N	**-$**	**-$**	**-$**
U Net Annual Savings	**=$**	**=$**	**=$**

V Use other side for Explanations, Comments, Rationales, Sources, Contacts, NIE Calculations, Etc. KEY REMARKS TO APPROPRIATE BLOCKS	**W** ______________________ ______ Prepared By Date

Attachment 3

Appendix C:
An Approach to
Business Continuity and Contingency Planning

Forward (Rev. 1 -- 01-26-01)

This document is intended as an approach to business continuity and contingency planning. It has been designed for use by the Medicare business partner system security officer (SSO) charged with preparing a business continuity and contingency plan or with updating an already existing plan.

The approach outlined in the following pages has been designed to provide information on which workable business continuity and contingency plans can be developed and implemented. This document is not all-inclusive nor is it intended to suggest that this is the only approach to contingency planning. Using these guidelines should spare business partner management and the systems security officer the necessity of devising alternate methods and will permit them to develop a basic and workable business continuity and contingency plan.

1. Introduction (Rev. 1 -- 01-26-01)

Introduction to Business Continuity and Contingency Planning

All Medicare business partners must prepare and annually review business continuity and contingency plans. Such plans outline the actions to take before, during, and after a disaster or major disruption to assure the continuity of key business systems and operations. Emergencies include fires, floods, storms, earthquakes, civil disorders, power failures, injuries, explosions, and bomb threats.

Business continuity planning identifies business-critical functions, resources and sets priorities for them. The contingency planning process then addresses all the resources needed to perform a business function and the means of implementing these resources. The following table provides guidelines in developing the business continuity portion of the contingency plan.

Business Continuity Planning	Requirement	Implementation
Critical Business Function Analysis & Prioritization		
1. Mapping critical Medicare business functions to major applications	Contingency Plan	Applications and data criticality
2. Mapping applications to technologies (platforms, LANs/WANs, data storage, imaging, EDI, etc.)	Contingency Plan	Applications and Data criticality
3. Impact of business cycle on prioritization (end of month, quarter-end, year-end, etc.)	Contingency Plan	Applications and data criticality
4. Strategy for regular update and review	Contingency Plan	Testing and revision
5. Clear statement of risk assumption	Contingency Plan	Applications and data criticality
6. Definition of minimum acceptable level of service and detailed actions to get to that level	Contingency Plan	Risk Assessment Applications and data criticality
7. Management participation and signoff on Medicare prioritization recommendations	Contingency Plan	Disaster Recovery Plan Emergency Mode Operations Plan Applications and data criticality

Planning for emergencies is done in three phases: response, backup, and recovery. Emergency response plans relate to the occurrence as it is happening and show how to protect lives, limit damage, protect sensitive data, and minimize the impact on operations. Backup plans relate to the period immediately after the occurrence, identifying vital (time-critical) operations and specifying the resources and temporary facilities necessary to assure their continuity until operations return to normal. Recovery plans assure the orderly resumption of all operations to full capacity in permanent quarters. Recovery plans must be coordinated with backup plans to assure that the transition is smooth and that there is no unresolved conflict.

A comprehensive contingency plan addresses:

- Business Continuity
- Personnel

- Data
- Software
- Hardware
- Communications
- Supplies
- Space and

Documentation

Although a business continuity and contingency plan is formulated under the guidance of the systems security officer (SSO), all organizational components are actively involved in providing information and making decisions.

2. Organizational Participation (Rev. 1 -- 01-26-01)

Business Partner Management

- Authorizes preliminary contingency planning;
- Ensures that all business components participate in the development of the Business Continuity and Contingency Plan;
- Reviews the plan and recommendations;
- Approves the Business Continuity and Contingency Plan; and
- Funds approved recommendations.

The Systems Security Officer (SSO)

- Explains the scope and purposes of contingency planning
- Reconciles discrepancies and conflicts;
- Evaluates security of backup sites;
- Prepares preliminary business continuity and contingency plan;
- Recommends additional safeguards or research;
- Submits the plan and recommendations to management;
- Schedules the implementation of approved measures; and
- Monitors implementation through participation in the Change Control Board.

Service Components (provide support functions such as maintenance, physical security, etc.)

- Schedule fire drills, and monitor effectiveness;
- Show how physical security forces respond to emergencies;

- Describe emergency re-supply procedures for forms, supplies, equipment, and furniture;
- Describe procedures for priority replacement of computer hardware;
- Describe procedures for restoring telecommunications;
- Describe procedures for backup sites and procedures;
- Provide information for the availability of recovery sites;
- Describe procedures on developing inventories of equipment and furniture;
- Provide a list of employees’ home address and phone numbers; and
- Describe procedures to ascertain availability of funds for backup and recovery.

Operating Components (IS operations personnel)

- Designate employees for emergency response teams;
- Designate employees for backup teams;
- Designate employees for recovery teams;
- Provide a list of employees' home addresses and telephone numbers;
- Identify vital (time-critical) operations/systems;
- Identify special needs such as vital forms/hardware;
- Validate inventories;
- Identify the data to be backed up offsite;
- Provide information on testing requirements;
- Identify vital (time-critical) non-ADP operations; and
- Review basic service-component plans and advise SSO where own needs are not met.

3. Preliminary Contingency Plan Development (Rev. 1 -- 01-26-01)

The Preliminary Contingency plan provides guidance as to what to do in case of disasters or disruptions. Make separate recommendations for safeguards, procedures, or decisions that can not be immediately implemented at the working level with available funds. For example, include nominations for response, backup, and recovery teams, but do not schedule or perform training. Instead, make practical recommendations showing management what is needed and why. Incorporate into the preliminary contingency plan existing procedures and any new procedures that can be developed easily and without higher approval; these are subject to review when the plan is submitted to management. Submit the preliminary contingency plan for management's approval with a cover memo giving an overview of the organization's preparedness, and include recommendations and justifications for additional safeguards and procedures; recommend further study of any safeguard where preliminary analysis is insufficient for a decision.

The preliminary plan consists of three phases:

- Response
- Backup
- Recovery

Each phase consists of a general plan that applies to the whole organization, followed by specific plans that apply to each component. First, develop each general plan with the service components and use that plan to show individual components what is done for them and what remains for them to do. Include with each component's plan the lists that apply to that component only, e.g., lists of their employees' home addresses and phone numbers, lists of forms and supplies vital to their operations. However, make attachments of general or bulky material such as inventories or interoffice directories.

1. Phase One – Response: Emergency response plans show how the organization responds to specific mishaps to protect lives, limit damage, protect sensitive data, and minimize the impact on operations. They deal separately with each type of disaster or disruption, showing what must be done and who must do it. For example, the overall plan lists the phone numbers of police/fire/ambulance, emergency control center, health unit, security officer, and safety manager; instructions for dealing with each emergency include the names and numbers of those to be notified. For example:

- Small, local fires easily contained: Put out fire and notify the safety manager, x87654.
- Fires in danger of spreading or producing noxious fumes: First, pull the alarm to evacuate the building, dial 911, describe the emergency (fire) and give the address and location. Then call the emergency control center x87653 and state that 911 has been called and reported the fire; give the address and location of the fire. Emergency control center employees meet the fire trucks and guide them to the proper location.
- Illness or injury: Call the nurse x87652, state the problem, the location and go to the elevator, wait for the nurse and direct the nurse to the patient. The nurse dials 911 to summon an ambulance, if indicated.
- Civil disorder, unruly demonstrations, vandalism, sabotage, illegal strikes, job actions: (As with each type disaster/disruption, including those listed below, the SSO finds out what the established procedure is and writes it down so that employees know who to contact and what to do.).
- Bomb threat and search
- Storms posing imminent danger
- Earthquakes
- Explosions
- Power, heating, and air conditioning failures

All components list the names, home addresses and phone numbers for their employees, distributing this information only to those designated to notify, inform and instruct them. Also, list the names of employees nominated for emergency response teams. Indicate which employees have responsibility for various decisions and notifications, and which are proficient in CPR, first aid, and fire extinguishing. Display emergency instructions and phone numbers (police, fire, guard, nurse, etc.) in each component and make sure that all employees know where they are posted; this is the first item any auditor should check when reviewing emergency response preparedness. Emergency response also includes prearranging with the local fire department(s) the following safety control responsibilities for handling emergencies:

- Who will respond;
- What is the best way to enter during and after working hours;
- Who will direct firemen to the fire;
- Where the data processing area is located;
- What kind of area fire extinguishing system the computer room has;
- Where the controls for any smoke-exhaust systems are located and who should activate them and under what conditions; and
- Where the tape library is and what equipment/chemicals/ procedures the firemen will use to prevent damage to the data contained on the tapes and disks.

Provide procedures to allow emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas. The following list of coded actions helps structure inputs and suggests what components need do to cooperate with authorities:

601 Identify the kind of emergency
602 Notify the designated authorities and report incident to HCFA CCMO
603 Assess the severity of emergency
604 Evacuate nonessential personnel (or all)
605 Summon inside aid and stand by to direct
606 Summon outside aid and stand by to direct
607 Protect EDP IT systems and data
608 Protect non-EDP IT data
609 Protect computer facilities
610 Protect mini-micro computer facilities
611 Protect remote workstations and links
612 Protect ancillary facilities
613 Protect office equipment and supplies
614 Guard site during emergency
615 Secure site after emergency
616 Notify insurance companies
617 Estimate damage
618 Estimate delay in operations
619 Notify all employees of the situation and what to do
620 Activate backup plans, if required
621 Activate recovery plans, if required
622 Salvage useable equipment and supplies

623 Clean up the premises
624 Report actions taken to management
625 Revise the emergency response plan per experience

Ask component representatives to consider "who, how, and why" when reviewing the checklist, to keep in mind the various kinds of emergencies that may arise, and to be aware of the roles played by service components and others. For example, action 602 could suggest notifying the component's emergency response team to extinguish a small fire, which in turn suggests that team members should be nominated, listed in the appendix, and recommended for special training in handling fire extinguishers. Action 614 raises the question of component responsibility for guarding the work area during various emergencies. Action 618 suggests that some criteria be developed for estimating delay in restoring operations, and action 619 asks how employees are informed of an off-hours emergency (by radio, phone). Action 620 raises the question of who makes the decision to activate backup plans, and which operations are actually vital, meaning time-critical; is an estimated 5-day delay acceptable, or must some operations be resumed in 3 days at the latest? The coded actions may also suggest preparations that require the cooperation or assistance of others, and it is the responsibility of the component to make such needs known to the SSO.

2. Phase Two – Backup: The service component indicates what backup facilities and storage are available to the organization, including pertinent details on how quickly the facilities become available and how long they remain available. This information is developed by the SSO before individual components are contacted for their inputs. Components are then acquainted with existing backup information to help them estimate their needs. Component representatives meet with their people to identify vital (time-critical) operations. These are the operations that cannot wait for recovery facilities to become available and useable, so components have to be advised how long it is likely to take before normal operations can resume. Designate any operation vital if it cannot be down over 5 working days without unacceptable degradation of mission.

Operating components are vitally concerned with backup determinations, being the part of the organization best acquainted with their own needs, and often the most knowledgeable of existing alternate facilities, such as suitable computer workstations located elsewhere in the network. Computer operations have special backup considerations having to do with equipment availability and compatibility, and the extensive site preparation often involved in recovery operations. Recommendations for alternate operating facilities made in the preliminary effort should suggest that a cost-benefit analysis first be made similar to the kind performed in risk analysis. However, offsite storage of vital data is obviously essential and worthwhile, whether such data is in the form of magnetic tape, floppy disc, cartridge, cassette, hardcopy, etc. Do not overlook projects-in-process, especially where working papers may represent months of effort.

The following list of coded actions suggest what might have to be done to assure continuity of vital (time-critical) operations:

701 Alert the backup processing facility
702 Activate the backup team and diary operations
703 Determine where processing was interrupted
704 Notify the backup processing facility

705 Move backup tapes/forms/supplies and secure
706 Recompile, copy tapes and return offsite
707 Test the backup equipment operations
708 Begin vital operations
709 Order forms/supplies according to project needs
710 Report processing problems to management
711 Revise the backup plan according to experience

The action code 702 suggests that certain employees be designated to take care of backup operations if any of the component's functions are vital (time-critical). If no function has been designated vital, note this fact on the sheet headed "Backup", and do not designate any backup team. Action 701 suggests contacting the backup facility at the first sign of trouble to prepare the manager for imminent notification; decide who alerts whom under what circumstances, and when to cancel the alert. Action 704 designates those authorized to reserve the facility under stated conditions. Action 705 suggests identifying critical tapes, supplies, and forms, storing them offsite in a location convenient to the backup processing site, and showing how these are transported and on whose authority. Give the authority's name, job title, and phone number. Action 710 suggests a procedure be established for keeping management apprised (including what to report and where to reach which managers). This indicates that management must know what is expected of the backup operation so that problem-reporting constitutes management-by-exception during this difficult period; problems show what is not being (or may not be) accomplished that should be.

3. Phase Three – Recovery: Resuming all operations can be a major undertaking that must be performed under pressure, whether it involves restoring existing facilities or relocating. There is always the possibility that recovery will have to be done in two stages and temporary (not backup) facilities occupied while damaged facilities are being renovated, or new facilities readied.

Describe the procedures service components use to locate facilities, provide physical security, and replace furniture, equipment, forms, and supplies. List the network of employees and suppliers through whom they work to supply the needs of the organization. Show how these procedures apply to disaster recovery. With such information, operating components can intelligently use the phase-three action plan to develop procedures that facilitate their own recovery operations. The following list of coded actions suggests what might have to be done to become fully operational once more:

801 Activate the recovery team and diary operations
802 Set-up recovery headquarters
803 Assess site damage with insurance adjusters
804 Fund/schedule restoration or relocation
805 Check EDP IT systems and data against inventory
806 Check non-EDP IT data against inventory
807 Check computer facilities against inventory
808 Check mini-micros against inventory
809 Check remote workstations against inventory
810 Check ancillary facilities against inventory

811 Check office equipment/supplies against inventory
812 Assess all non-site damage with adjusters
813 Fund/schedule repairs and replacements
814 Schedule return of furloughed employees
815 Test EDP IT equipment/operations
816 Coordinate recovery/backup operations
817 Reduce backlog of non-vital operations
818 Revise recovery plan according to experience

Action 801 indicates that certain employees are designated to perform certain recovery tasks. They should not be the same ones who are designated to perform backup operations. This may pose a perplexing resource-allocation problem for computer operations. Address it well ahead of the need. By definition, recovery sites are not reserved ahead of time, so Action 802 suggests that suitable recovery headquarters be listed from which recovery operations might be directed. Service components can assist in this once they know how many executives to accommodate and what their needs are. Service components should also be aware of whatever alternate premises are generally available that would accommodate the entire organization. This may involve contacting local real-estate brokers to determine what suitable premises are usually available in the area, including hotels and motels. The SSO must meet several times with the service components and operating components to develop the preliminary contingency plan.

Should there be any questions as to what categories 805 through 811 consist of, copy the breakdown shown in the Risk Assessment, Appendix B, take an inventory of your Medicare assets, and give it to component representatives assisting in contingency planning. The inventories referred to are the official ones developed and maintained by service components and attached to the contingency plan.

Actions 804 and 813 indicate that advance consideration should be given to the availability of funds for recovery. Consider gaps in insurance coverage for some of the named disasters before the fact and make management aware of the vulnerabilities in the summary, along with recommendations as to how to deal with them.

The SSO stresses the need to revise the plan according to experience. This implies that someone be assigned to keep track of each phase and note what works well and what doesn't so that the plan can be modified accordingly.

4. Implementing the Contingency Plan (Rev. 1 -- 01-26-01)

To assure full management participation in the decisions that guide the organization safely through periods of great stress, the preliminary plan is not considered implemented until approved and published.

The SSO prepares a cover memo transmitting both the plan and the recommendations to management. The memo briefly explains the goals of contingency planning and summarizes the strengths and weaknesses of the organization's preparedness. The recommendations are a separate attachment; they propose and estimate resources required for such initiatives as:

- Training

- Offsite storage for critical data
- Backup facilities
- Survey of potential recovery sites
- Review of insurance coverages
- Prioritizing computer operations
- Developing alternate site processing instructions
- Providing more/different fire extinguishers
- Installing sprinklers in critical areas

The success of the contingency plan depends on prompt review and implementation. The preliminary contingency plan becomes the contingency plan when it is fully implemented. This means the plan has been published and individual recommendations have been implemented, scheduled, or denied. For example, it is misleading to consider an organization without an implemented contingency plan because a sprinkler system needs to be costed out and installed. However, the SSO keeps track of the status of pending actions, advising management of progress and updating the contingency plan. Thus an auditor can review the implemented plan, can follow the rationale for not implementing safeguards that appear desirable, and can check on the status of those initiatives to which the organizations are committed. When the plan is implemented, make sure the employees know those parts that apply to them. Acquainting employees with the procedures is not considered formal training but merely a part of their ordinary responsibilities to be discussed with supervisors and periodically reviewed in staff meetings. Approved formal training warrants highest priority, particularly the training of emergency response teams.

Because the contingency plan "may burn up in the fire", store copies offsite where they can be accessed when needed. Secure a complete copy at the tape storage facility, and applicable sections elsewhere, such as the computer backup facility itself.

5. Attachments (Rev. 1 -- 01-26-01)

Collect existing material that facilitates response, backup, and recovery operations. Much of this material is bulky and relates to the entire organization. The SSO ensures that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the contingency plan. Such material includes:

- Master inventories of forms, supplies, and equipment
- Description of computer hardware and peripherals
- Computer software
- Systems and program documentation
- Prioritized schedules for computer operations
- Communications requirements, especially computer networks

6. Testing and Updating (Rev. 1 -- 01-26-01)

Annually review and update all three phases of the contingency plan. The SSO must follow up on the status of recommendations and show the date of the most recent revision on the cover page of each copy of the plan.

Test contingency plans to the extent feasible. If there are no computer backup facilities, take advantage of whatever testing privileges are offered contractually. If a reciprocal backup agreement is negotiated, make provision for reciprocal testing. Where such testing is not practicable, document the reasons and show how compatibility can be achieved at the time of need, and in what timeframes. Estimate daily processing hours relative to availability of the facilities.

Testing includes activities other than computer processing; attempt manual operations according to contingency plan procedures, and make changes as experience indicates. Conduct drills since they are a form of testing procedures. Practice the use of fire extinguishers, even though discharging them is impractical.

Conscientious review, discussion, and evaluation of plans with all concerned parties is essential and must be part of the initial planning and annual updates particularly concerning any changes being considered in the organization or operations. Where testing is prohibitive because of cost or disruption of operations, a critical walk-through of the plan may be substituted. Do the walk-through annually. Document each test or walk-through by a written report.

7. Outline of a Typical Business Continuity and Contingency Plan (Rev. 1 -- 01-26-01)

The following outline of a typical contingency plan may not be suitable for all organizations or operations, but serves as an example of an acceptable plan. Likely sources are indicated as service component, operating component or outside source:

1. <u>Management Summary and Recommendations</u>: (Service components, operating components) Also address business continuity issues here.

2. <u>Phase One: Response-</u>

- List of names and numbers to phone in various contingencies. (Service components)
- List of possible contingencies showing who to call for help and how employees should respond (Service components and outside sources such as police and fire departments):
  - Small fires that are local and easily contained
  - Any fire in danger of spreading or producing noxious fumes
  - Illness or injury
  - Civil disorder, unruly demonstrations, vandalism, sabotage, strike, job action, etc.
  - Bomb threat and search
  - Storms posing imminent danger

  - Earthquakes
  - Explosions
  - Power, heating, air-conditioning failures
- Coded actions indicating components' plans and involvement. (All components)
- List of names and home addresses and phone numbers of each component's employees. (All components)
- List of names of members of each component's emergency response team. (All components)

3. Phase Two: Backup-

- Backup agreements showing what facilities are available under what conditions and for how long. (Service components)
- Description of the facilities, equipment, and supplies needed for each component's vital operations. (All components)
- Coded actions indicating each component's plans and involvement. (All components)
- Lists of names of members of each component's backup team. (All components requiring backup operations)

4. Phase Three: Recovery-

- A statement showing the general availability of suitable facilities in the area, plus names and numbers of realtors to contact. (Service components, outside sources)
- A statement describing the processes used in securing new facilities, equipment and supplies, including names and numbers of those involved and the recovery functions and responsibilities of each. (Service components)
- Coded actions indicating each component's recovery plans and involvement. (All components)
- Lists of names of members of each component's recovery team. (All components)

5. Record of Recommendations: Approval, denial, and implementation schedule. (Management and all components)

6. Attachments: Complete equipment inventories, lists of computer software, systems and program documentation, prioritized computer schedules, list of all forms, list of all supplies, copy of current office directory, and lists of communications requirements, especially relating to computer networks. (Service components and operating components)

7. Record of Testing and Updating: (Service components and operating components)

Appendix D:
An Approach to Fraud Control

1. Introduction (Rev. 1 -- 01-26-01)

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. Safeguards Against Employee Fraud (Rev. 1 -- 01-26-01)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These are consistent with the HCFA Core Security Requirements outlined in Appendix A of the HCFA 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 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 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 himself 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's 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. Checklist for Medicare Fraud (Rev. 1 -- 01-26-01)

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 identifying 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 Personnel department check the applicant's background, employment record, references, and possible criminal record before hiring?

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

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

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

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

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

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

30) Are special fraud controls specified for backup operations?

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

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

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

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

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

Appendix E: (Rev. 1 -- 01-26-01) 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
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

HCFA	**Health Care Financing Administration**
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 (HCFA)**
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	**HCFA 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	Standard 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 F: (Rev. 1 -- 01-26-01)
Glossary

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

Term	Definition
Application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. (FISCAM)
Application Controls	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. (FISCAM)
Application Programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities. (FISCAM)
Application Programs	See Application.
Application System(s)	A computer system written by or for a user that applies to the user’s work; for example, a payroll system, inventory control system, or a statistical analysis system. (AISSP) (FIPS PUB 11-3)
Application System Manager	See Application Manager.
Asset	Any software, data, hardware, administrative, physical communications, or personnel resource within an ADP system of activity.
Attack	The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (NCSC-TG-004)
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (NSTISSI)
Audit 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.

Term	Definition
Backup	Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource. (FISCAM)
Backup Plan	See Contingency Plans.
Batch (Processing)	A mode of operation in which transactions are accumulated over a period of time, such as a day, week, or month and then processed in a single run. In batch processing, users do not interact with the system while their programs and data are processing as they do during interactive processing. (FISCAM)
Biometric Authentication	The process of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometric devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. (FISCAM)
Breach(es)	The successful and repeatable defeat of security controls with or without an arrest, which if carried to consummation, could result in a penetration of the system. Examples of breaches are: 1. Operation of user code in master mode. 2. Unauthorized acquisition of identification password or file access passwords. 3. Accessing a file without using prescribed operating system mechanisms. 4. Unauthorized access to tape library.
Browsing	(1) The act of electronically perusing files and records without authorization. (FISCAM) (2) The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (NCSC-TG-004)
Business Partners	Non-federal personnel who perform services for the federal government at a site owned by the partner under the terms and conditions of a contractual agreement. Business partners need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements. HCFA business partners are Standard Systems Maintainers (SSM), CWF host sites, DMERC, Data Centers and other specialty contractors.
Certification (Recertification)	(1) Consists of a technical evaluation of a sensitive application to see how well it meets security requirements. (AISSP) (FIPS PUB 102) (2) A formal process by which an agency official verifies, initially or by periodic reassessment, that a system's security features meet a set of specified requirements.
Checkpoint	The process of saving the current state of a program and its data, including intermediate results to disk or other nonvolatile storage, so that if interrupted the program could be restarted at the point at which the last checkpoint occurred. (FISCAM)
Chief Information Officer (CIO)	The **CIO** is responsible for the implementation and administration of the AIS Security Program within an organization.

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

Term	Definition
Computer Security	See Information Systems Security and Systems Security.
Computer Security Incident Response Capability (CSIRC)	That part of the computer security effort that provides the capability to respond to computer security threats rapidly and Effectively. [A CSIRC provides a way for users to report incidents, and it provides personnel and tools for Investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents.] (AISSP) (Source: NIST SPEC PUB 800-3)
Computer System	(1) A complete computer installation, including peripherals, in which all the components are designed to work with each other. (FISCAM) (2) Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (AISSP) (Computer Security Act of 1987)
Confidentiality	Ensuring that transmitted or stored data are not read by unauthorized persons. (FISCAM)
Configuration Management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. (FISCAM)
Console	Traditionally, a control unit such as a terminal through which a user Communicates with a computer. In the mainframe environment, a **Console** is the operator's station. (FISCAM)
Consortium	Currently consists of four HCFA offices (Northeastern, Southern, Midwestern, and Western) that oversee the operations at the Regional Offices.
Consortium Contractor Management Officer (CCMO)	Part of the Regional Consortiums, the **CCMO** is responsible for leading and directing contractor management at the consortium level.
Contingency Plan(s)	(1) Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster. (FISCAM) (2) A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (AISSP) (FIPS PUB 11-3)
Contingency Planning	(1) The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. (ISSPH - Glossary) (2) See contingency plan. (FISCAM)

Term	Definition
Contractors	Non-federal personnel who perform services for the federal government under the terms and conditions of a contractual agreement. Contractors need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.
Control Technique	Statements that provide a description of what physical, software, procedural or people related condition must be met or in existence in order to satisfy a core requirement. (Appendix A.)
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text or plain text and other data are transformed into coded form by encryption and translated back to plain text or data by decryption. (FISCAM)
Data	Facts and information that can be communicated and manipulated. (FISCAM)
Data Administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. (FISCAM)
Data Center	See Computer Facility.
Data Communications	(1) The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM) (2) The transfer of data between functional units by means of data transmission according to a protocol. (AISSP) (FIPS PUB 11-3)
Data Control	The function responsible for seeing that all data necessary for processing 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 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)

Term	Definition
Data Security	(1) The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (FIPS PUB 39) (2) See Security Management Function.
Data Validation	Checking transaction data for any errors or omissions that can be detected by examining the data. (FISCAM)
Database	(1) A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer. (FISCAM) (2) A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (AISSP) (FIPS PUB 11-3)
Database 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)
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)

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

Term	Definition
Firewall	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. (FISCAM)
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. (FISCAM)
General Controls	The structure, policies, and procedures that apply to an entity's overall computer operations. They include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls. (FISCAM)
General Support System(s) (GSS)	(1) An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a **general support system** is to provide processing or communication support. (FISCAM) (2) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (SSPS&GH - Glossary)(Source: OMB Circular A-130)
Guided Media	(1) Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable) (2) Provides a closed path between sender and receiver • Twisted Pair (e.g. Telephone cable) • Coaxial Cable • Optical Fiber (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
Handled	(As in "Data handled.") Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.
Hardware	The physical components of information technology, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. (FISCAM)
Image	An exact copy of what is on the storage medium
Implementation	The process of making a system operational in the organization. (FISCAM)

Term	Definition
Incident	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.
Information	(1) The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people. (FISCAM) (2) Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (AISSP) (OMB Circular A-130)
Information Resource	See Resource.
Information Resource Owner	See Owner.
Information Systems (IS)	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (NSTISSI)
Information Systems Security (INFOSEC)	The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including cryptosecurity, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (AISSP) (NISTIR 4659) (Also see Systems Security)
Information Systems Security Officer (ISSO)	(1) Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer. (NSTISSI)
Information Technology (IT)	(1) Processing information by computer. (TechEncy) (2) IT or Information Technology has probably been the most redefined term over the past few years. The definition has varied from simple automation of manual processes using micro-processors to computers to networks to desktop publishing to networking. (Source: U. Texas)
Initial Program Load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program. (FISCAM)
Input	Any information entered into a computer or the process of entering data into the computer. (FISCAM)
Integrity	With respect to data, its accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users. (FISCAM)
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user. (FISCAM)

Term	Definition
Internal Control	A process, effected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. **Internal control** also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring. (Also referred to as Internal Control Structure) (FISCAM)
Internet	When capitalized, the term "**Internet**" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
Investigation(s)	The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system.
IPL	See Initial Program Load.
Job	A set of data that completely defines a unit of work for a computer. A **job** usually includes programs, linkages, files, and instructions to the operating system. (FISCAM)
Junk Mail (e-mail)	Transmitting e-mail to unsolicited recipients. U.S. federal law 47USC227 prohibits broadcasting junk faxes and e-mail, allowing recipients to sue the sender in Small Claims Court for $500 per copy. (TechEncy)
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message. (FISCAM)
Key Management	Supervision and control of the process whereby a key is generated, stored, protected, transferred, loaded, used, and destroyed. (NSTISSI)
Keystroke Monitoring	A process whereby computer system administrators view or record both the keystrokes entered by a computer user and the computer's response during a user-to-computer session. (AISSP – Source: *CSL Bulletin*)
Library	In computer terms, a **library** is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a **library**, each program is called a member. **Libraries** are also called partitioned data sets (PDS). **Library** can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape **libraries**. (FISCAM)

Term	Definition
Library Control/Management	The function responsible for controlling program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. (FISCAM)
Library Management Software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes. (FISCAM)
Life-Cycle Process **Life-Cycle Model**	(1) Spans the entire time that a project/program including hardware and software is being planned, designed, developed, procured, installed, used, and retired from service. (2) A framework containing the processes, activities and tasks involved in the development, operation and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use. (Source: ISO/IEC 12207)
{PRIVATE**}Limited Background Investigation (LBI)**	This investigation consists of a NACI, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years. (SSPS&GH - Glossary)
Load Library	A partitioned data set used for storing load modules for later retrieval. (FISCAM)
Load Module	The results of the link edit process. An executable unit of code loaded into memory by the loader. (FISCAM)
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)

Term	Definition
Mail Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system. (TechEncy)
Mainframe System (Computer)	A multi-user computer designed to meet the computing needs of a large organization. The term came to be used generally to refer to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations. (FISCAM)
Maintenance	(1) Altering programs after they have been in use for a while. **Maintenance** programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time. (FISCAM) (2) The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions. (Source: IEEE Std 610.12-1990)
Major Application (MA)	(1) OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application. (FISCAM) (2) An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A major application can be either a major software application or a combination of hardware/software. Its sole purpose is to support a specific mission-related function. (ISSPH - Glossary) (3) An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB Circular A-130) All "Major Applications" require "special management attention." The System Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.
Malicious Software (Code)	The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (AISSP – Source: DHHS Definition, adapted from NIST SPEC PUB 500-166)

Term	Definition
Master Console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands. (FISCAM)
Master File(s)	In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period. (FISCAM)
Material	Refers to data processed, stored, or used in and information generated by an ADP system regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements.
Media	The physical object such as paper, PC, and workstation diskettes, CD-ROMs, and other forms by which HCFA 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. (SSPS&GH)
Methodology	The specific way of performing an operation that implies precise deliverables at the end of each stage. (TechEncy)
Migration	A change from an older hardware platform, operating system, or software version to a newer one. (FISCAM)
Minimum Background Investigation (MBI)	This investigation includes a NACI, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. The MBI is an enhanced version of the NACIC and can be used for selected public trust positions.
Mission Critical	Vital to the operation of an organization. In the past, mission critical information systems were implemented on mainframes and minicomputers. Increasingly, they are being designed for and installed on personal computer networks. (TechEncy)
Misuse of Government Property	The use of computer systems for other than official business that does not involve a criminal violation but is not permissible under HCFA policies. (SSPS&GH - Glossary)
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. (SSPS&GH - Glossary)

Term	Definition
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. Small or large, a computer network exists to provide computer users with the means of communicating and transferring information electronically. (AISSP – Source: *Microsoft Press Computer Dictionary*)
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)	HCFA Office that ensures the effective management of HCFA's information systems and resources. The office also develops and maintains central data bases and statistical files, and directs Medicare claims payment systems.
On-line	Available for immediate use. It typically refers to being connected to the Internet or other remote service. When you connect via modem, you are online after you dial in and log on to your Internet provider with your username and password. When you log off, you are offline. With cable modem and DSL service, you are online all the time. A peripheral device (terminal, printer, etc.) that is turned on and connected to the computer is also online. (TechEncy)
Operating System(s) (OS)	The master control program that runs the computer. It is the first program loaded when the computer is turned on, and its main part, called the kernel, resides in memory at all times. It may be developed by the vendor of the computer it's running in or by a third party. (TechEncy)
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy. (FISCAM)
Owner	Manager or director with responsibility for a computer resource, such as a data file or application program. (FISCAM)
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs. (FISCAM)

Term	Definition
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). (SSPS&GH - Glossary)
PDS	See Partitioned Data Set.
Penetration	Unauthorized act of bypassing the security mechanisms of a system. (NSTISSI)
Penetration Test	An activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.
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)
Project Officer	HCFA 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)

Term	Definition
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)
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)

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

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

Term	Definition
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)
Security Management Function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness. (FISCAM)
Security Plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. (FISCAM)
Security Policy	The set of laws, rules, and practices that regulate how an Organization manages, protects, and distributes sensitive information. (NCSC-TG-004)
Security Profile	See Profile.
Security Program	An entitywide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. (FISCAM)
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (NSTISSI)
Security Requirements Baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security. (NSTISSI)

Term	Definition
Security Software	See Access Control Software.
Sensitive Application	An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (AISSP – Source: OMB Circular A-130)
Sensitive Data	Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (AISSP – Source: OMB Circular A-130)
Sensitive Information	(1) Any information that, if lost, misused, or accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. (FISCAM) (2) **A**ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (AISSP – Source: Computer Security Act of 1987) (3) **A**ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under E-Mail 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (ISSPH - Glossary) (Source: Computer Security Act of 1987)
Sensitivity of Data	The need to protect data from unauthorized disclosure, fraud, waste, or abuse. (SSPS&GH)
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network. (FISCAM)
Service continuity controls	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (FISCAM)
Significant Change	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (AISSP – Source: DHHS Definition)

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

Term	Definition
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)
System	(1) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (OMB Circular A-130) (2) Refers to a set of information resources under the same management control that share common functionality and require the same level of security controls. • The phase "General Support Systems (GSS)" as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications (MA)," as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, control software, or software for command and control). By categorizing both "General Support Systems" and "Major Applications" as "systems", unless explicitly stated, the procedures and guidance can address both in a simplified manner. • When writing the required System Security Plans, two formats are provided--one for General Support Systems, and one for Major Applications. This ensures that the differences for each are addressed (HCFA, 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)
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)

Term	Definition
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 HCFA security policy or lead to a fraudulent act or criminal violation through use of an HCFA system. (SSPS&GH – Glossary)
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)
Technical Controls	See Logical Access Control.

Term	Definition
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)
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)
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)
Unclassified	Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (NSTISSI)

Term	Definition
UNIX	A multitasking operating system originally designed for scientific purposes which has subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. **UNIX** is also a major server operating system in the client/server environment. (FISCAM)
Update Access	This access level includes the ability to change data or a software program. (FISCAM)
User	(1) The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) (2) Any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (AISSP – Source: OMB Circular A-130)
User Identification (ID)	A unique identifier assigned to each authorized computer user. (FISCAM)
User Profile	A set of rules that describes the nature and extent of access to each resource that is available to each user. (FISCAM)
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)
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (FISCAM)
Virus	(1) A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. (FISCAM) (2) A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. (NCSC-TG-004)
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	NIST Special Publication 800-12 Footnote 131: The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. The ambiguity results from the fact that current laws were written years before such concerns as keystroke monitoring or system intruders became prevalent. Additionally, no legal precedent has been set to determine whether keystroke monitoring is legal or illegal. System administrators conducting such monitoring might be subject to criminal and civil liabilities. The Department of Justice advises system administrators to protect themselves by giving notice to system users if keystroke monitoring is being conducted. Notice should include agency/organization policy statements, training on the subject, and a **banner** notice on each system being monitored. [NIST, *CSL Bulletin*, March 1993]
Wide Area Network (WAN)	(1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) (2) A communications network that connects geographically separated areas. (AISSP – Source: *Microsoft Press Computer Dictionary*)
Workstation	A microcomputer or terminal connected to a network. **Workstation** can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability. (FISCAM)
Worm	(1) An independent computer Program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. (FISCAM) (2) A program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information. (AISSP – Source: *Microsoft Press Computer Dictionary*)
Write	Fundamental operation in an IS that results only in the flow of information from a subject to an object. (NSTISSI)
Write Access	Permission to write to an object in an IS. (NSTISSI)

References:

1. NCSC-TG-004 **–** Rainbow Series, Aqua Book, **"*Glossary of Computer Security Terms*",** NCSC-TG-004-88, Library No. S-231,238**.** Issued by the National Computer Security Center (NCSC).
2. FISCAM – Federal Information System Controls Audit Manual, GAO/AIMD-12.19.6
3. 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.
4. AISSP – "Automated Information Systems Security Program Handbook", DHHS, http://wwworim.nih.gov/policy.assip.html, (for Source references see document)
5. SSPS&G Handbook – Systems Security Policy Standards and Guidelines Handbook – (Formerly the HCFA INFORMATION SYSTEMS SECURITY PROGRAM (ISSP) Handbook, June 30,2000).
6. HISM - Handbook of Information Security Management *(Imprint: Auerbach Publications) (Publisher: CRC Press LLC)*Authors: Micki Krause, Harold F. Tipton ISBN: 0849399475
7. DoN **-** Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A, Aug. 3,1982. (Glossary)
8. NSTISSI – National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999 (Revision 1)
9. TechEncy – Technical Encyclopedia of definitions supported by TechWeb.com