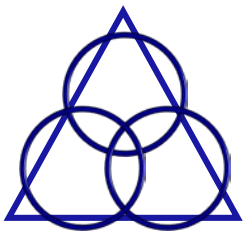
IS Auditing 101

NEIAF June 18, 2015



United States Government Accountability Office

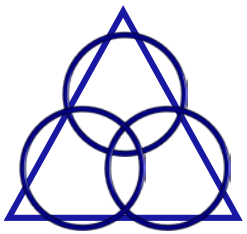
GAO

February 2009

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)

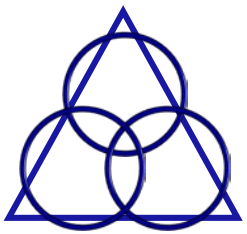
GAO-09-232G

http://www.gao.gov/fiscam/overview



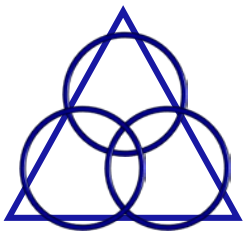
Planning

- Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit
- Understand the Entity's Operations and Key Business Processes.
- Obtain a General Understanding of the Structure of the Entity's Networks
- Identify Key Areas of Audit Interest
- Assess Information System Risk on a Preliminary Basis
- Identify Critical Control Points
- Obtain a Preliminary Understanding of Information System Controls



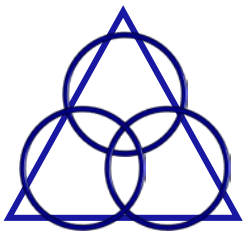
Planning

- Perform Other Audit Planning Procedures
  - Relevant Laws and Regulations
  - Previous Audits and Attestation Engagements
  - Audit Resources
  - Communication with Entity Management and Those Charged with Governance
  - Service Organizations
  - Using the Work of Others



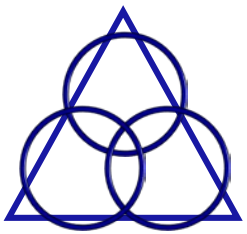
Planning

- Documentation
- Electronic listing of
  - users,
  - user ID,
  - last logon date,
  - role/access rights
- Sample of employee personnel files
- Sample configuration changes (system and/or application) and emergency changes
- Sample vendor agreements



Entrance Conference

- Criteria
- Access to and security of records
- Access to key personnel
- If applicable, unannounced site visits
- Prompt notification of findings
- Reporting



NIST

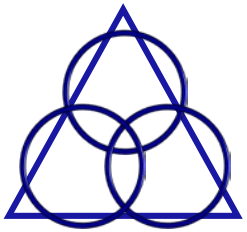
http://csrc.nist.gov/publications/PubsSPs.html

SPECIAL PUBLICATIONS (800 SERIES)

Special Publications in the 800 series (established in 1990) are of general interest to the computer security community. This series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

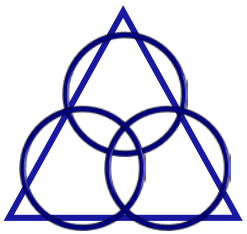
[Publications that link to ***dx.doi.org/...*** will redirect to another NIST website. See more details about DOIs.]

Number	Date	Title
SP 800-171 (Draft)	Nov. 18, 2014	**DRAFT Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations** Announcement and Draft Publication
SP 800-170	June 2014	**2013 Computer Security Division Annual Report** SP 800-170 - Annual Report (2013) FAQ doi:10.6028/NIST.SP.800-170 [Direct Link]
SP 800-168	May 2014	**Approximate Matching: Definition and Terminology** SP 800-168 FAQ doi:10.6028/NIST.SP.800-168 [Direct Link]
SP 800-167 (Draft)	Aug. 22, 2014	**DRAFT Guide to Application Whitelisting** Announcement and Draft Publication
SP 800-165	Jun 2013	**2012 Computer Security Division Annual Report** Annual Report (2012) - SP 800-165 FAQ doi:10.6028/NIST.SP.800-165 [Direct Link]
SP 800-164 (Draft)	Oct. 31, 2012	**DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices** Announcement and Draft Publication
SP 800-163 (Draft)	Aug 19, 2014	**DRAFT Technical Considerations for Vetting 3rd Party Mobile Applications** Announcement and Draft Publication



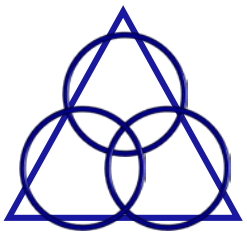
NIST

- 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- 800-12 An Introduction to Computer Security: The NIST Handbook



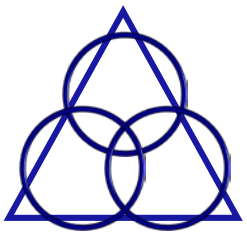
Laws and Regulations

- Federal Information Security Management Act of 2002 44 U.S.C. § 3541 - FISMA
- Federal Financial Management Improvement Act of 1996, 31 U.S.C. 3512 - FFMIA
- Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. 3512 (c), (d) - FMFIA
- OMB, *Management of Federal Information Resources*, Circular A-130
- OMB, *Management's Responsibility for Internal Control*, Circular A-123
- OMB, *Financial Management Systems*, Circular A-127,
- Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 - HIPAA



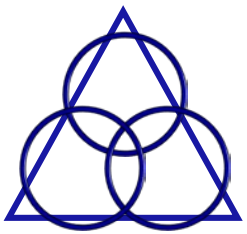
Laws and Regulations

- Gramm-Leach-Bliley Act, Pub. L. 106-102 (Nov. 12, 1999
- Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. 108-173 - MMA
- OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy,* 39
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information*, and40
- OMB Memorandum M 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*



Laws and Regulations

- In IS audits of state and local governments, the auditor should identify applicable legal and reporting requirements and issues.



Information System Controls: Security Objectives

- Confidentiality
- Integrity
- Availability

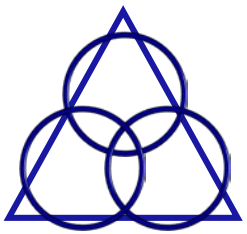
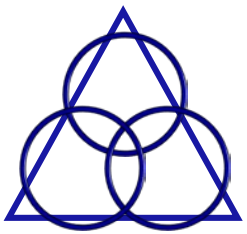
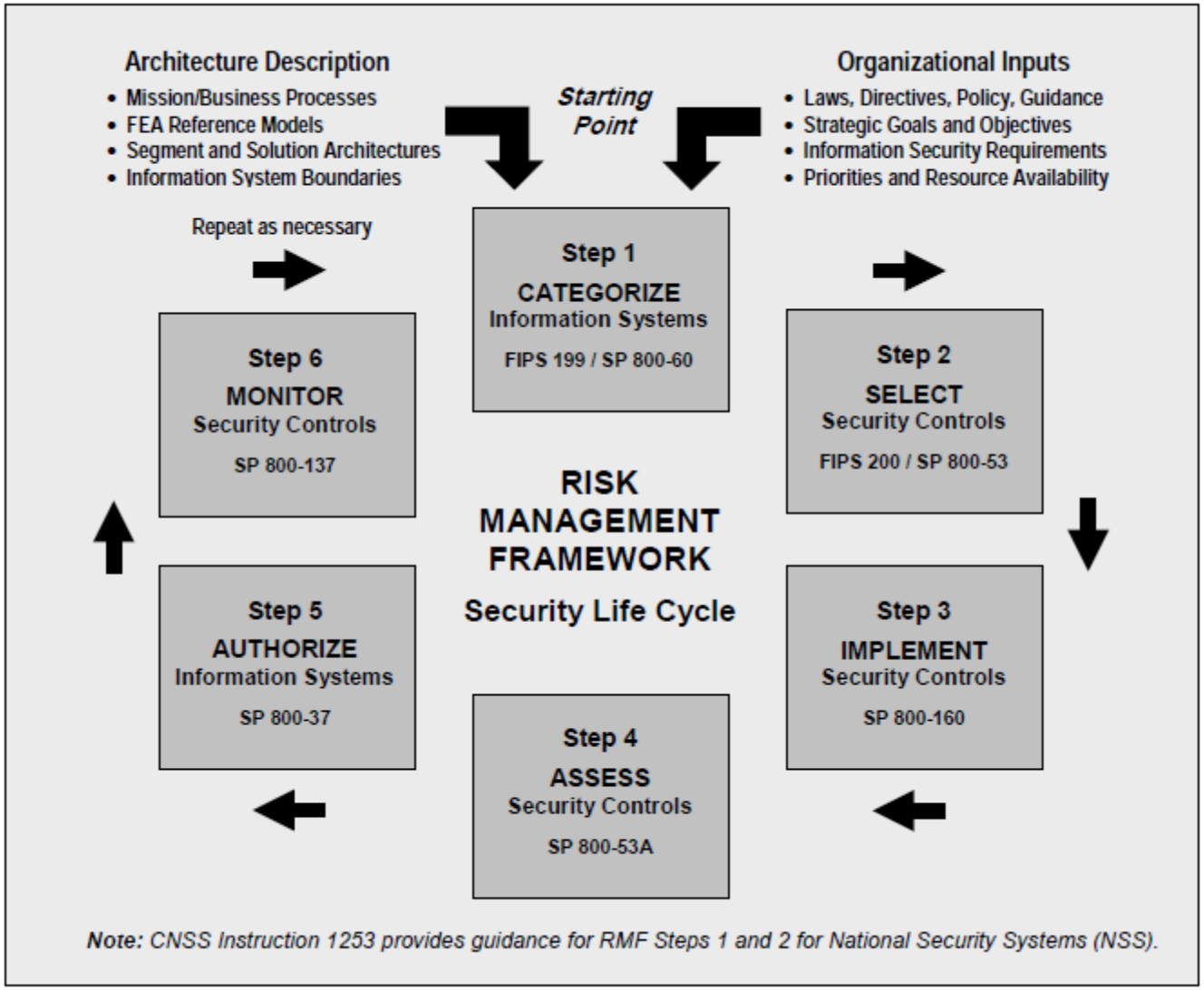


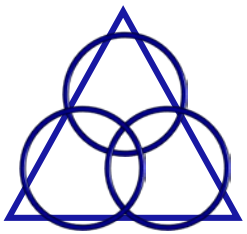
Table 1 summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

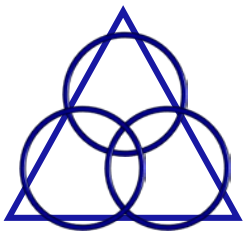



Architecture Description
• Mission/Business Processes
• FEA Reference Models
• Segment and Solution Architectures
• Information System Boundaries
Starting Point
Organizational Inputs
• Laws, Directives, Policy, Guidance
• Strategic Goals and Objectives
• Information Security Requirements
• Priorities and Resource Availability
Repeat as necessary
Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60
Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53
Step 3
IMPLEMENT
Security Controls
SP 800-160
Step 4
ASSESS
Security Controls
SP 800-53A
Step 5
AUTHORIZE
Information Systems
SP 800-37
Step 6
MONITOR
Security Controls
SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).



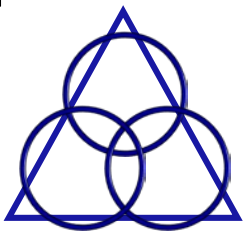
Reporting

- Findings should not be a surprise to the auditee
- Note any corrective action taken or planned
- Note impact
  - Confidentiality
  - Integrity
  - Availability



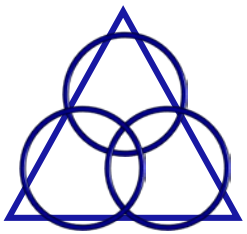
Reporting

- FISMA requires federal agencies to report significant deficiencies in information security as material weaknesses under FMFIA and, if relating to financial management systems, as an instance of a lack of substantial compliance of systems with FFMIA.
- For FISMA, OMB defines the term *significant deficiency* as “a weakness in an agency’s overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.



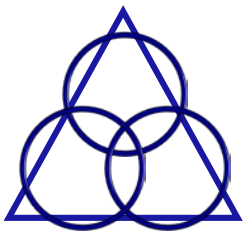
Reporting

- Control the dissemination of the report
- DO NOT post on the internet
- Possibly exempt from FOIA requests – check with your agency



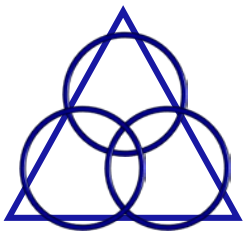
Controls

- General
- Business Process Application



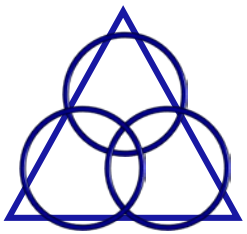
General

- Security Management
- Access Controls
- Configure Management
- Segregation of Duties
- Contingency Planning



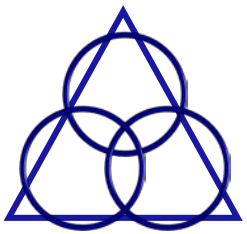
Business Process Application

- Application Level General Controls
- Business Process Controls
- Interface Controls
- Data Management Systems Controls



Security Management

- Establish a security management program
- Periodically assess and validate risks
- Document and implement security policies and procedures
- Implement security awareness and other personnel policies
- Monitor the effectiveness of the security program
- Effectively remediate information security weaknesses
- Ensure activities performed by external parties are secure

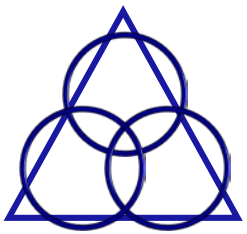


The Tour

- Want to see anything and everything that has to do with Information Systems
  - Data center
  - Back-up site
  - Media Disposal
  - Generators/Battery back-up
  - Network Closets
- Observe
- Test
- Interview
- Inspect
- Surreptitious Entry

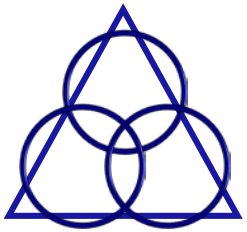
Access Controls

- Adequately protect information system boundaries.
- Implement effective identification and authentication mechanisms.
- Implement effective authorization controls.
- Adequately protect sensitive system resources.
- Implement an effective audit and monitoring capability.
- Establish adequate physical security controls.



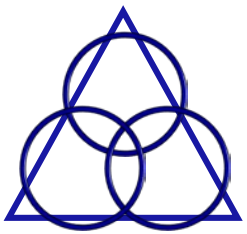
Configuration Management

- Develop and document CM policies, plans, and procedures.
- Maintain current configuration identification information.
- Properly authorize, test, approve, track, and control all configuration changes.
- Routinely monitor the configuration.
- Update software on a timely basis to protect against known vulnerabilities.
- Appropriately document and approve emergency changes to the configuration.



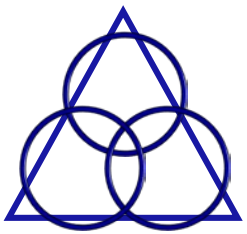
Segregation of Duties

- Segregate incompatible duties and establish related policies.
- Control personnel activities through formal operating procedures, supervision, and review.



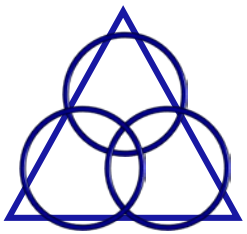
Contingency Planning

- Assess the criticality and sensitivity of computerized operations and identify supporting resources.
- Take steps to minimize potential damage and interruptions.
- Develop and document a comprehensive contingency plan.
- Periodically test the contingency plan and adjust it as appropriate.



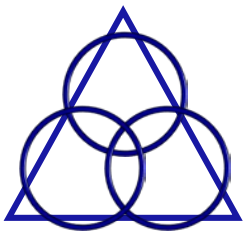
Application Level General Controls

- Implement effective application security management.
- Implement effective application access controls.
- Implement effective application configuration management.
- Segregate application user access to conflicting transactions and activities and monitor segregation.
- Implement effective application contingency planning.



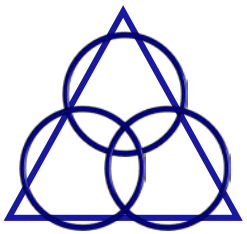
Business Process Controls

- Transaction data input is complete, accurate, valid, and confidential.
- Transaction data processing is complete, accurate, valid, and confidential.
- Transaction data output is complete, accurate, valid, and confidential.
- Master data setup and maintenance is adequately controlled.



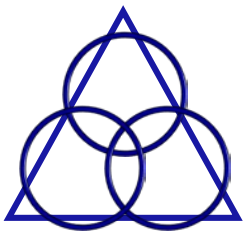
Interface Controls

- Implement an effective interface strategy and design.
- Implement effective interface processing procedures.



Data Management System Controls

- Implement an effective data management system strategy and design.



You will receive an e-mail regarding today's session. Please respond to the course evaluation and survey.

Thank you for attending today.

NEIAF Executive Committee