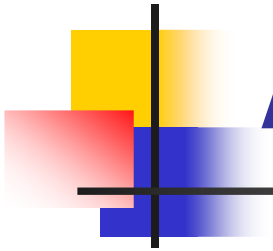
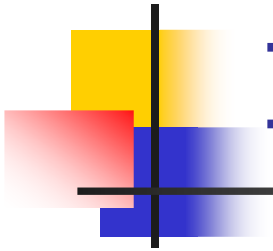
NIST 800-53A: Guide for Assessing the Security Controls in Federal Information Systems

Samuel R. Ashmore
Margarita Castillo
Barry Gavrich



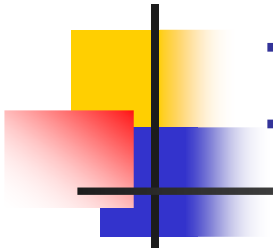
Assessing Security Controls

- Introduction
- Framework and Methods
- Assessment Process
- Assessment Procedures
- Assessment Expectations
- Sample Assessment
- References
- Questions



Introduction

- Security Assessments Performed Throughout System Development Life Cycle (SDLC) Phases
  - System initiation
  - Development and acquisition
  - Implementation
  - Operational and maintenance
  - Disposal
- Assessments Performed Relative to System Risk, Minimally on an Annual Basis, A-130

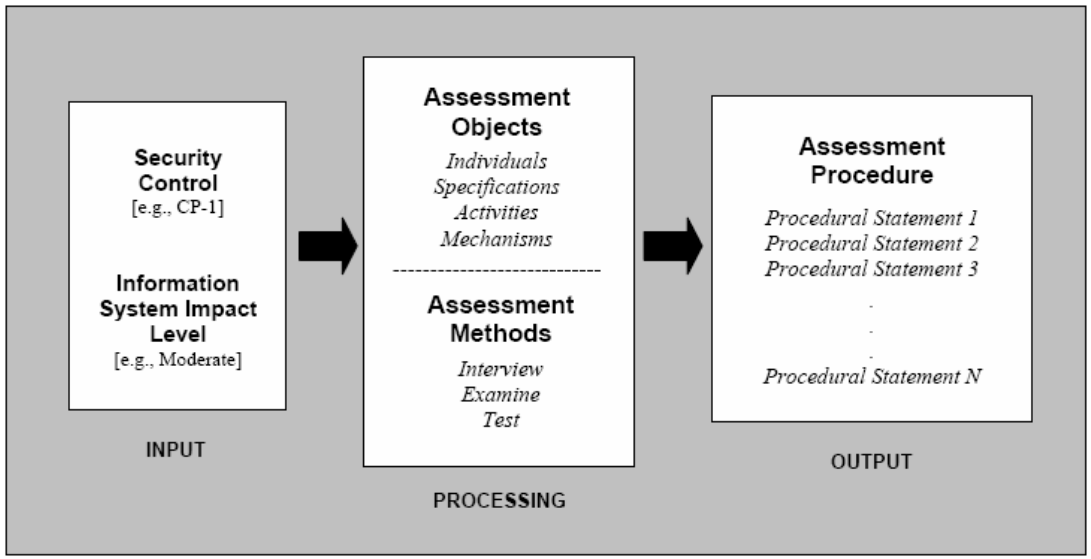


Introduction

- Security Control Types:
  - Management
  - Operational
  - Technical safeguards
- Rely on Additional Input From:
  - Security categorization from SP800-53 / FIPS 199
  - Level of assurance required for operation
- Additional Assessment Documents
  - SP800-37, Guide for Security C&A
  - Common Criteria, FIPS 140-2

Framework of Assessment Procedures

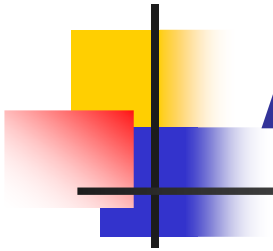
- Framework: Input, Processing, and Output
  - Input: 800-53, and FIPS 199
  - Policy, procedures, security requirements
  - Specific protection-related actions
  - Specific items: hardware, software, firmware



Framework cont

- Formal Discussions to Understand and Clarify
- Review, Inspect, Observe an Assessment Object
- Testing Exercises Assessment Objects to Compare Actual with Expected Behavior
- Determination of Overall Security Effectiveness

ASSESSMENT METHODS: Interview, Examine, Test		**INFORMATION SYSTEM IMPACT LEVEL**		
ATTRIBUTE	VALUE	LOW	MODERATE	HIGH
Depth (Interview and examine methods only)	Generalized	√	---	---
	Focused	---	√	---
	Comprehensive	---	---	√
Type (Test method only)	Functional (black-box)	√	√	√
	Penetration	---	√	√
	Structural (gray-box, white-box)	---	---	√
Coverage (All methods)	Number and types of assessment objects determined by organizations in collaboration with assessors.	√	√	√



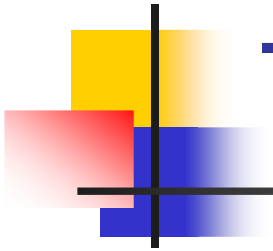
Assessment Procedures

- Security Control is Described by its Functionality
- Assessment Procedure is Developed Using Procedural Statements
  - Low-impact
  - Medium-impact
  - High-impact
- Procedural Statements Build Upon Previous
  - Hierarchical form

Assessment Procedure Catalog

- Format of Assessment Procedures

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	CP-5 CONTINGENCY PLAN UPDATE Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	✓	✓	✓
CP-5.1	***Examine*** *organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually.*	✓	✓	✓
CP-5.2	***Examine*** *the contingency plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.*		✓	✓
CP-5.3	***Examine*** *organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan update control is implemented.*		✓	✓
CP-5.4	***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis.*			✓



The Process

- Security Assessment Plans
  - Identify controls and enhancements to be assessed
  - Assessment procedures and steps
  - Develop additional assessment procedures
  - Optimize procedure selection to minimize duplication
    - Not covered in SP800-53, or requiring additional IA
  - Review and reuse of previous assessment results
    - Applicability of previous assessments
  - Finalize and obtain approval to use the plan
    - Key milestones in the assessment process
  - Document, analyze, monitoring, apply results

Assessment Procedure Catalog

- Catalog of Assessment Procedures for NIST 800-53 Security Controls
- 17 Assessment Procedure Categories Organized in "Families" Similar to 800-53
  - Primary procedural statement followed by unique identifier (e.g., CP-3.2) indicating secondary procedural statement(s)
  - Statements are organized hierarchically by information system impact level ranging from low, to moderate, to high

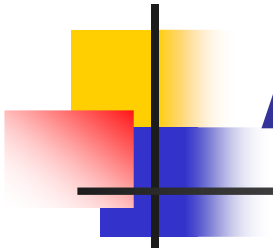
Procedural Statements

- Statements Identify Assessment Method(s) to be used for the Security Control
- Statement Categories Organized into Family (e.g., Access Control) and 3 Classes (Technical, Operational, Management)
- Category Listing Includes NIST 800-53 Step Number, and FIPS Assessment Procedure (e.g., Low, Moderate, High)

NIST 800-53 Structure

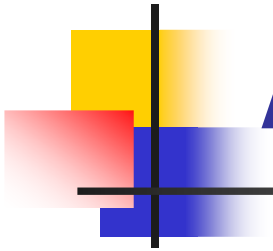
CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS



Access Control

- AC-2 Account Management
- AC-10 Concurrent Session Control
- AC-13 Supervision and Review
  - User activities are supervised and reviewed with respect to enforcement and usage of information systems access controls by the organization
- AC-16 Automated Labeling
- Least Privilege, Unsuccessful Login Attempts, Wireless Access Restrictions



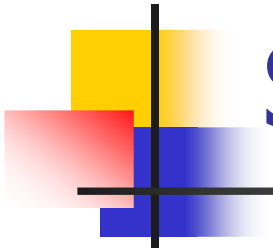
Awareness and Training

- AT-1 Security Awareness and Training Policy and Procedures
- AT-2 Security Awareness
- AT-3 Security Training
- AT-4 Security Training Records
- AT-5 Contacts with Security Groups and Associations
  - Purpose is to network with special interest groups, specialized forums and professional associations to remain up-to-date with recommended security practices, techniques and technologies

Audit and Accountability

- AU-8 Time Stamps
- AU-9 Protection of Audit Information
  - Audit information and audit tools are protected by the information system from unauthorized access, modification, and deletion
- AU-10 Non-Repudiation
- AU-11 Audit Retention
- Auditable Events, Contents of Audit Records, Audit Storage Capacity

Certification, Accreditation, and Security Assessment



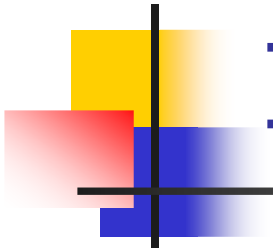
- CA-2 Security Assessments
- CA-3 Information System Connections
- CA-5 Plan of Action and Milestones
- CA-6 Security Accreditation
- CA-7 Continuous Monitoring
  - The organization is required to monitor the security controls in the information system on an on-going basis

Configuration Management

- CM-2 Baseline Configuration and System Component Inventory.
- CM-3 Configuration Change Control
- CM-5 Access Restrictions for Change
  - Enforcement of physical and logical access restrictions associated with change to the information system recording related events
- CM-7 Least Functionality

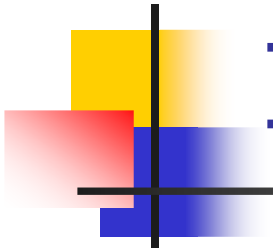
Contingency Planning

- CP-3 Contingency Training
- CP-4 Contingency Plan Testing
- CP-6 Alternate Storage Sites
- CP-9 Information System Backup
  - User-level and system-level information contained in the information system are routinely backed-up and stored at an appropriately secure location



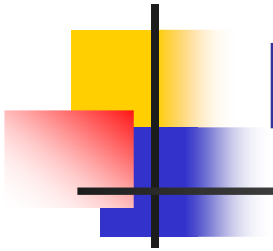
Identification and Authentication

- IA-1 Identification and Authentication Policy and Procedures
- IA-3 Device Identification and Authentication
- IA-4 Identifier Management
  - Organization manages user identifiers by:
    - Uniquely identifying each user
    - Verifying user identity
    - Receiving authorization to issue user identifier from an appropriate organization official
    - Disabling user identifier after period of inactivity
    - Archiving user identifiers



Incident Response

- IR-3 Incident Response Testing
- IR-4 Incident Handling
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
  - Incidents and relevant information are promptly reported to appropriate authorities
- Incident Response Policy and Procedures, Incident Response Assistance



Maintenance

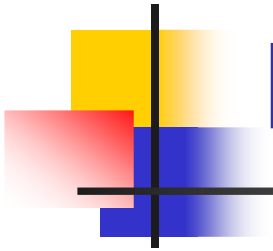
- MA-2 Periodic Maintenance
- MA-3 Maintenance Tools
  - Approval, control and monitor of information system tools and tool maintenance
  - Media containing diagnostic test programs are checked for malicious code before use
- MA-4 Remote Maintenance
- Maintenance Personnel, Timely Maintenance

Media Protection

- MP-2 Media Access
- MP-4 Media Storage
  - Information system media is stored using physical controls and secure storage based on FIPS highest security category of the information recorded on the media
- MP-5 Media Transport
- MP-6 Media Sanitation and Disposal

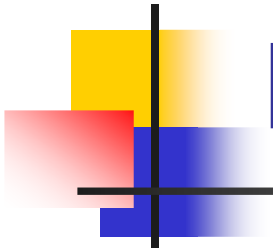
Physical and Environmental Protection

- PE-8 Access Logs
  - Visitor access logs to facilities are maintained to include visitor name and organization, visitor signature, form of identification used, date of access, time of entry / departure, purpose of visit, name and organization of person visited
- PE-10 Emergency Shutoff
- PE-16 Delivery and Removal
- PE-18 Location of Information System Components



Planning

- PL-3 System Security Plan Update
- PL-4 Rules of Behavior
  - Set of rules describing user responsibilities, and expected behavior with regard to information and information system usage
  - Signed acknowledgement from users indicating they have read, understood and agree to abide by the rules before access is granted to user
- PL-5 Privacy Impact Assessment
- PL-6 Security-Related Activity Planning

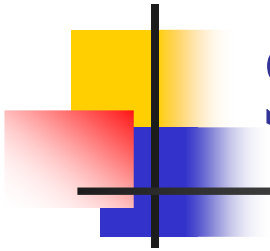


Personnel Security

- PS-2 Position Categorization
- PS-3 Personnel Screening
- PS-4 Personnel Termination
- PS-5 Personnel Transfer
  - Reviews information system / facilities access authorizations when individuals are reassigned or transferred to other positions with organization and initiates appropriate actions (e.g., reissue keys, identification cards etc.)

Risk Assessment

- RA-2 Security Categorization
- RA-3 Risk Assessment
  - Organization conducts assessments of risk, and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency
- RA-4 Risk Assessment Update
- RA-5 Vulnerability Scanning
  - List of information system vulnerabilities are kept up-to-date.



System and Services Acquisition

- SA-3 Life Cycle Support
- SA-6 Software Usage Restrictions
- SA-7 User Installed Software
  - Enforcement of explicit rules governing the downloading and installation of software by users
- SA-8 Security Design Principles
- Life Cycle Support, Outsourced Information System Services, Developer Configuration Management

System and Communications Protection

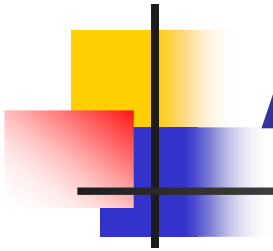
- SC-2 Application Partitioning
  - Separation of user functionality and information system functionality
- SC-3 Security Function Isolation
  - Information system isolates security functions from non-security functions
  - Information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both non-security functions and other security functions
- SC-4 Information Remnants
- SC-5 Denial of Service Protection

System and Information Integrity

- SI-2 Flaw Remediation
- SI-3 Malicious Code Protection
- SI-4 Information System Monitoring Tools and Techniques
- SI-6 Security Functionality Verification
  - The information system verifies the correct operation of security functions upon system startup and restart, upon user command with appropriate privilege, notifies system administrator, shuts the system down, restarts the system, when anomalies are discovered

Assessment Expectations

- Based on Categorization of the System
  - Low
    - Controls are in place
      - No obvious errors
  - Medium
    - Controls are thought out, operation has been verified
  - High
    - Controls continuously updated

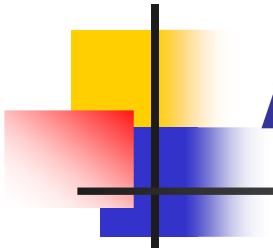


Assessment Example, pt 1.

- Low Impact System
- Contingency Planning
  - Examine policy
  - Examine records
    - Check for records of backup
  - Insure plans have been distributed

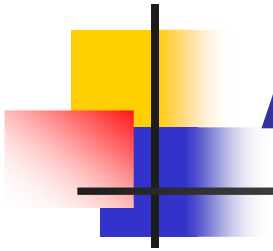
Assessment Example, pt 2.

- Medium Impact System
- Contingency Planning
  - Check Policy makes sense
  - Policy is reflective of current vulnerabilities
  - Policies contain specific actions
  - If roles are specified, then roles are updated with personal changes
  - Insure personal are trained for their roles



Assessment Example, pt 2.

- Contingency Planning cont.
  - Insure the plans are tested on a regular basis
  - Insure tests cover all areas of the plan
  - Insure adjustments are made from tests
  - Insure agreements are in place for backup sites
  - Check for documentation of vulnerabilities at primary location



Assessment Example, pt 2.

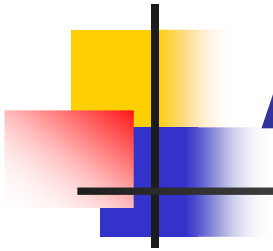
- Contingency Planning cont.
  - Check backup communication
    - Ensure availability
    - No shared vulnerabilities
  - Insure information to be backed up is defined
  - Insure a schedule and roles are defined
  - Check that information is tested after backup

Assessment Example, pt 2.

- Contingency Planning cont.
  - Examine media for compliance to policy
  - Proper record keeping
  - Interview personal to ensure familiarity with compliance

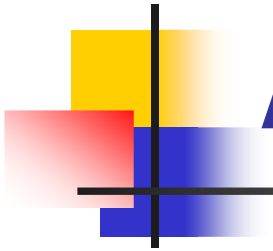
Assessment Example, pt 3.

- High Impact
- Contingency Planning
  - Check policy makes sense
  - Policy is reflective of current vulnerabilities
  - Policies contain specific actions
  - Clearly define roles and roles are updated with personal changes
  - Continuously updates
  - Insure personal are trained for their roles



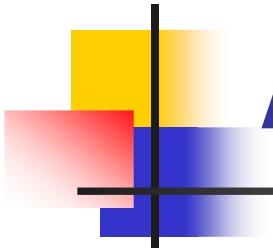
Assessment Example, pt 3.

- Contingency Planning cont.
  - Document anomalies, and use them to update plan
  - Insure plan is updated at least once a year
  - Insure lessons learned are use in update
  - Check if contingencies are practiced at all sites
  - Check if the results of practices are used to update plans



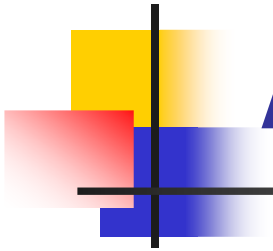
Assessment Example, pt 3.

- Contingency Planning cont.
  - Insure tests cover all areas of the plan
  - Insure adjustments are made from tests
  - Insure agreements are in place for backup sites
  - Check for documentation of vulnerabilities at all location
  - Check if agreements are reviewed on a regular basis.



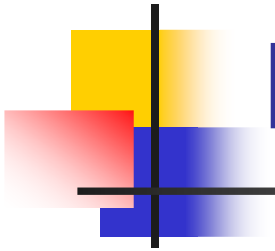
Assessment Example, pt 3.

- Contingency Planning cont.
  - Check backup communication
    - Ensure availability
    - No shared vulnerabilities
  - Insure information to be backed up is defined
  - Insure a schedule and roles are defined
  - Check that information is tested after backup
  - Examine media for compliance to policy



Assessment Example, pt 3.

- Contingency Planning cont
  - Proper record keeping
  - Interview personal to ensure familiarity with all aspects of the above policy
  - Interview personal about effectiveness of policy
  - Test all contingency plans
  - Test backup site
  - Test data recovery



References

- Federal Information Security Management Act (FISMA), Dec 2002
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Nov 2000
- Federal Information Processing Standards (FIPS)
  - FIPS 140-2: Cryptographic Modules, May 2001
  - FIPS 199: Security Categorization of Federal Information and Information Systems, Feb 2004
  - FIPS 200: Minimum Security Requirements of Federal Information and Information Systems, Mar 2006
- SP800-30: Risk Management Guide for IT Systems, Jul 2002
- SP800-37: Guide for C&A of Federal Information Systems, May 2004
- SP800-53: Revision 1, Recommended Security Controls for Federal Information Systems (Draft), Mar 2006
- Government Accountability Office (GAO) Federal Information Controls Audit Manual, Jan 1999