

NIST Special Publication 800-53A

Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans

UCDMO Conference

September 1-2, 2009

Dr. Ron Ross

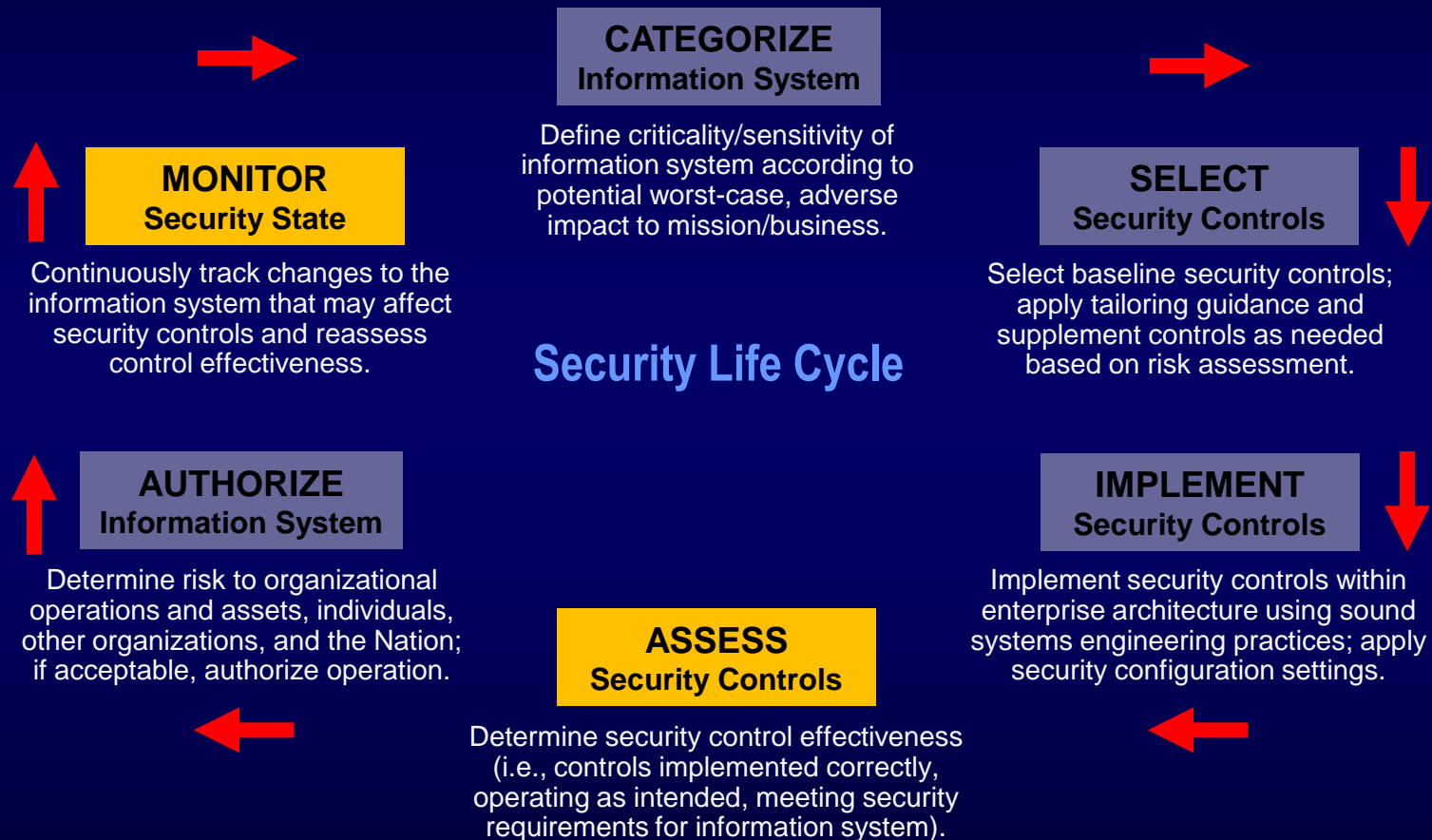
*Computer Security Division
Information Technology Laboratory*

Purpose

- Provide guidelines for building effective security assessment plans and procedures to enable assessment of security controls.
- Support the Risk Management Framework at the *assess* and *monitor* security control steps.

Risk Management Framework

Starting Point



Security Control Requirements

- *What security controls are needed to adequately protect an information system that supports the operations and assets of the organization?*
 - Categorize the system to determine potential impact of a breach of **confidentiality, integrity** and **availability**.
 - Select controls following **NIST SP 800-53** and (if applicable) companion document for national security systems, **CNSSI 1253**.

Security Control Effectiveness

- *To what extent are the security controls implemented correctly, operating as intended, and producing the desired outcome with respect to meeting information security requirements?*
 - Assess implemented controls following guidance in NIST SP 800-53A.
 - Determine security control effectiveness and acceptance of mission/business function risk to the organization.

Security Control Assessments

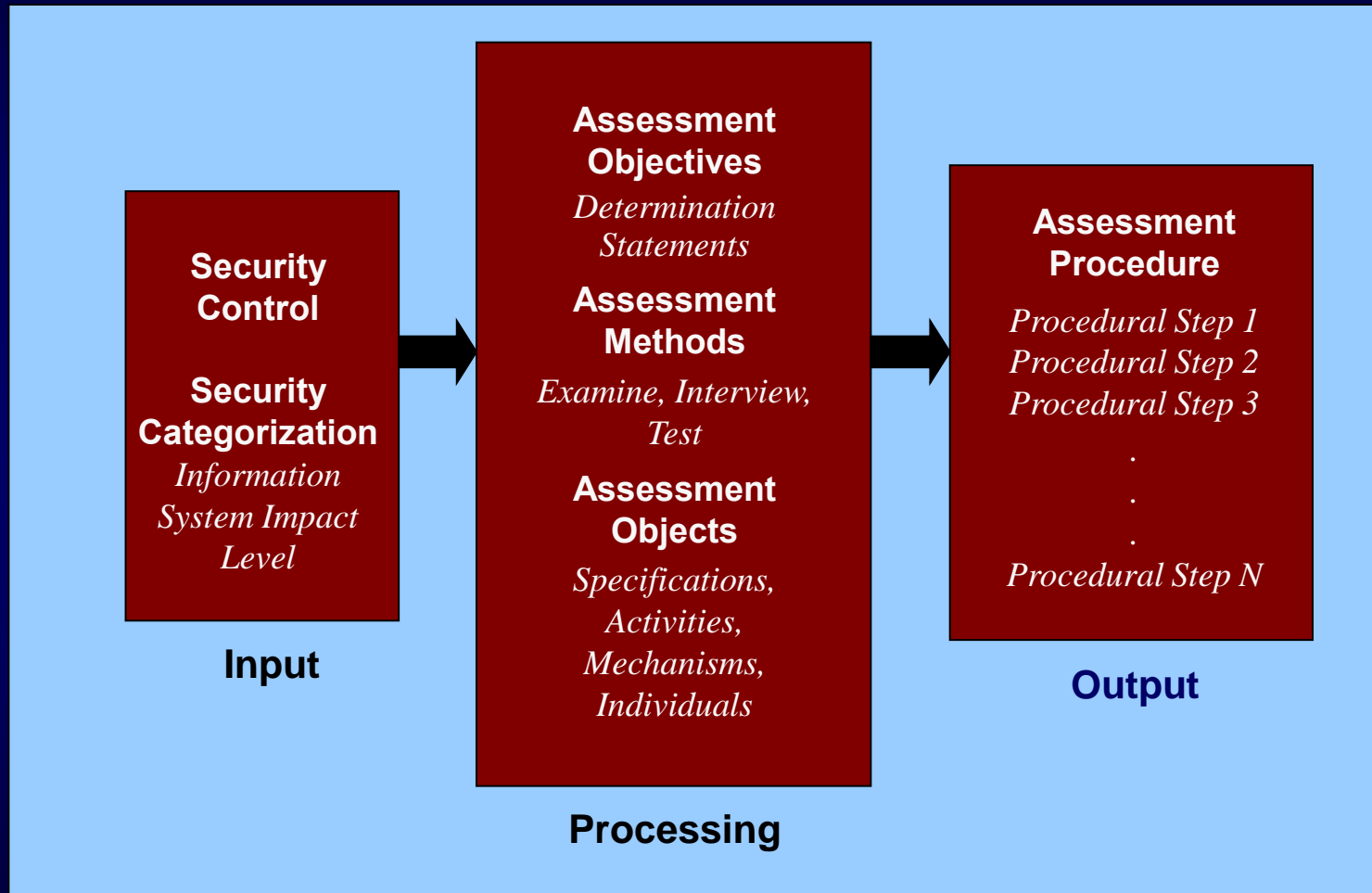
- Identify potential problems or shortfalls in the organization's implementation of the Risk Management Framework;
- Identify information system weaknesses and deficiencies;
- Prioritize risk mitigation decisions and associated risk mitigation activities;
- Confirm that identified weaknesses and deficiencies in the information system have been addressed; and
- Support information system authorization decisions, budgetary decisions, and the capital investment process.

Significant Benefits

- More consistent, comparable, and repeatable security control assessments.
- More cost-effective security assessments contributing to the determination of overall control effectiveness.
- More complete, reliable, and trustworthy information for organizational officials—to support information sharing, authorization decisions, and FISMA compliance.

Security Control Assessments

Conceptual Framework



Pre-Assessment Preparation

Approved
System
Security
Plan

Organization Preparation

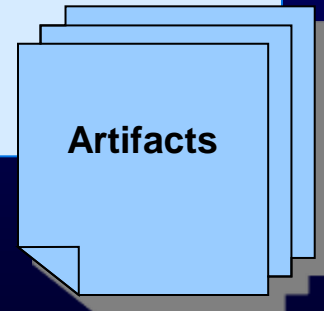
- Implement the security controls in the information system.
- Notify key organizational officials of impending assessment.
- Establish and open communications channels among stakeholders.
- Identify and allocate necessary assessment resources; assemble assessment team.
- Establish key milestones to effectively manage the assessment.
- Assemble artifacts for assessment

Pre-Assessment Preparation

Approved
System
Security
Plan

Assessor Preparation

- Establish appropriate organizational points of contact.
- Understand organization's mission, functions, and business processes.
- Understand information system structure (i.e., system architecture).
- Understand security controls under assessment and relevant security standards and guidelines.
- Develop security assessment plan.
- Obtain artifacts for assessment.



Preparing Assessment Plans

- Determine which security controls are to be assessed.
- Select appropriate procedures to assess the security controls.
- Tailor assessment procedures for specific operating environments.
- Develop assessment procedures for additional assurance requirements and optimize for maximum efficiency.
- Finalize security assessment plan and obtain approval to execute.

Assessment Procedure

- A set of procedural steps that are used to achieve one or more assessment ***objectives*** by applying specified assessment ***methods*** to specified assessment ***objects***.
- The application of an assessment procedure to a security control produces assessment ***findings***.
- Assessment findings are subsequently used in helping to determine the overall ***effectiveness*** of security controls employed in information systems.

Assessment Objectives

- A set of *determination statements* related to the particular security control under assessment.
 - Closely linked to the content of the security control (i.e., the security control functionality) and the assurance requirements in NIST Special Publication 800-53.
- Ensures traceability of assessment results to security control requirements.

Assessment Methods

- **Examine**
 - Process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects to facilitate assessor understanding, achieve clarification, or obtain evidence.
- **Interview**
 - Process of conducting discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence.
- **Test**
 - Process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.

Assessment Method Attributes

- Depth
 - Addresses rigor and level of detail in examination, interview, and testing processes.
 - Possible values: generalized, focused, and detailed.
- Coverage
 - Addresses scope or breadth of examination, interview, and testing processes
 - Number and type of objects and/or individuals to be examined, tested or interviewed.
 - Possible values: representative, specific, and comprehensive.

Assessment Objects

- Specifications
 - Document-based artifacts (e.g., policies, procedures, plans, functional specifications, architectural designs).
- Mechanisms
 - Hardware, software, and firmware safeguards (e.g., physical access control devices, I&A mechanisms, cryptographic mechanisms).
- Activities
 - Protection-related actions that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising contingency plan).
- Individuals
 - People applying the specifications, mechanisms, or activities.

Assessment Expectations

Assessment Expectations	Information System Impact Level		
	Low	Moderate	High
Security controls are in place with no obvious errors.	√	√	√
Increased grounds for confidence that the security controls are implemented correctly and operating as intended.	---	√	√
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	---	---	√
Grounds for a high degree of confidence that the security controls are complete, consistent, and correct. <i>Beyond minimum recommendations of Special Publication 800-53A</i>	<i>For environments with specific and credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets.</i>		

Types of Assessment Procedures

- Specialized Assessment Procedures
 - Unique to an individual security control or control enhancement.
 - Reflects the NIST Special Publication 800-53 requirement for assurance that the specified functionality within a security control or control enhancement has been implemented.
- Extended Assessment Procedure
 - Complements the specialized assessment procedures.
 - Reflects other aspects of the Special Publication 800-53 assurance requirements.
 - Organizations have discretion on how procedure is applied during an assessment (e.g., control, family, or assessment level).

Selection of Assessment Procedures

Depends on three factors:

- The security categorization of the information system;
- The security controls selected for implementation in the information system; and
- The level of assurance that the organization must have in determining the effectiveness of the security controls in the information system.

Example – Building the Procedure

- Security Control CP-1

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Specialized Assessment Procedure

(1 of 2)

CP-1.1

Assessment Objective:

Determine if:

- (i) the organization develops and documents contingency planning policy and procedures;*
- (ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;*
- (iii) responsible parties within the organization periodically review contingency planning policy and procedures; and*
- (iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.*

Assessment Methods and Objects:

Examine (depth, coverage): Contingency planning policy and procedures; other relevant documents or records.

Interview (depth, coverage): Organizational personnel with contingency planning and plan implementation responsibilities.

Specialized Assessment Procedure

(2 of 2)

CP-1.2

Assessment Objective:

Determine if:

- (i) *the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;*
- (ii) *the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and*
- (iii) *the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.*

Assessment Methods and Objects:

Examine (depth, coverage): Contingency planning policy and procedures; other relevant documents or records.

Interview (depth, coverage): Organizational personnel with contingency planning and plan implementation responsibilities.

Extended Assessment Procedure

EAP.1

Assessment Objective:

Determine if the organization has a process in place to address in a timely manner, any flaws discovered in the implementation or application of the security controls in the information system.

Assessment Methods and Objects:

Examine (depth, coverage): Policies, procedures, records, documents, activities, or mechanisms related to addressing flaws in security controls or control enhancements.

- EAP.1 applied to all information systems.
- Additional EAP steps applied selectively to moderate and high-impact information systems.
- EAP steps are hierarchical and cumulative.

Tailor Assessment Procedures

- Tailoring should take into account:
 - Assessment object-related considerations.
 - Depth and coverage-related considerations.
 - Common security control-related considerations.
 - System/platform and organization-specific considerations.
 - Reuse of assessment evidence-related considerations.
 - Information system impact-related considerations.
 - External information system-related considerations.

Reuse of Assessment Evidence

- Reuse of existing security assessment information can facilitate more efficient and cost-effective assessments.
- When considering the reuse of assessment results from previous assessments, assessors should validate:
 - the credibility of the evidence obtained;
 - the appropriateness of previous analysis; and
 - the applicability of the evidence to present information system operating conditions.
 - the amount of time that has transpired since the previous assessments.
 - the degree of independence of the previous assessments.

Guidance on Procedure Building

- NIST SP 800-53A Appendix F – Assessment Procedure Catalog.
 - Provides procedures for each security control listed in NIST SP 800-53.
 - *To be updated to align with NIST SP 800-53 Revision 3.*
- NIST SP 800-53A Appendix H – Assessment Procedure Worksheet.
 - Assists in identification and selection of base set of procedures.
 - *To be updated to align with NIST SP 800-53 Revision 3.*

Assessment Findings

- Are produced for each determination statement in a procedural step executed by an assessor
 - *Satisfied (S)*; or
 - *Other than satisfied (O)*.
- Provide visibility (through objective reporting) into specific weaknesses and deficiencies in the information system.
- Facilitate a disciplined and structured approach to mitigating risks based on organizational priorities.

Assessment Results

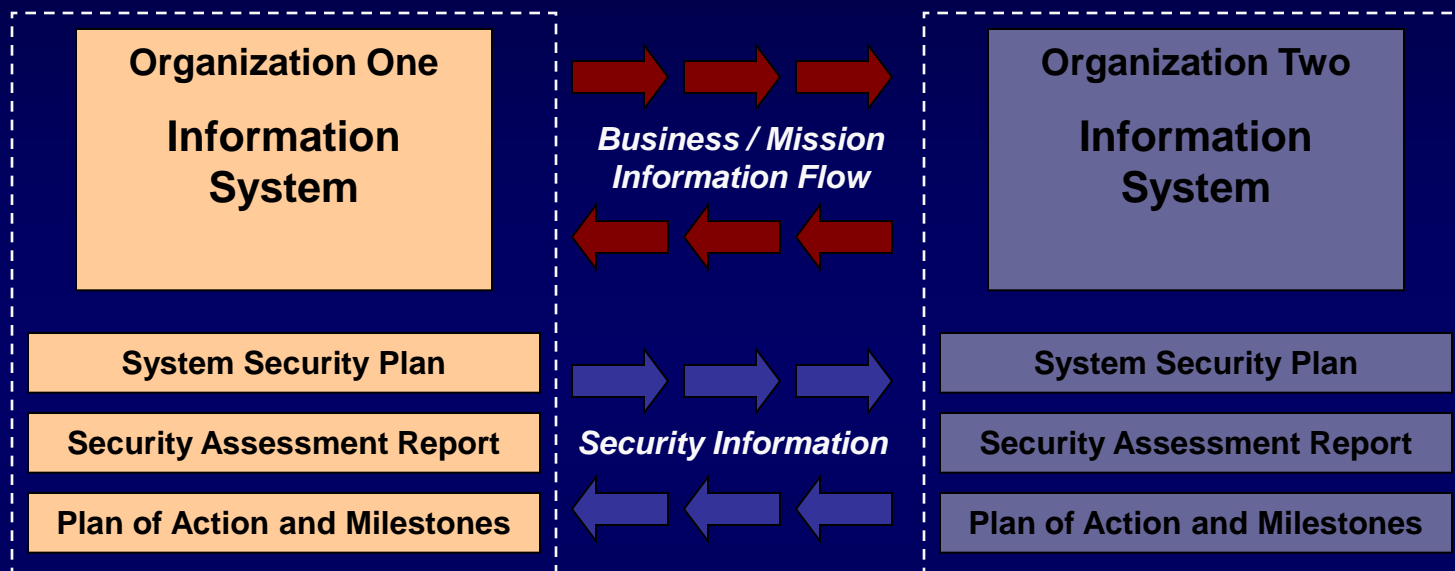
- The security assessment report generates updates to other key documents including:
 - System Security Plan;
 - Risk Assessment; and
 - Plan of Action and Milestones.
- Used by organizational officials to make decisions on the security state of the information system with respect to mission/business function risk.

Assessment Automation

- Information Security Automation Program (ISAP).
- Security Content Automation Protocol (SCAP).
- Web Support: <http://nvd.nist.gov/scap.cfm>

The Desired End State

Security Visibility Among Business/Mission Partners



Determining the risk to the first organization's operations and assets and the acceptability of such risk

Determining the risk to the second organization's operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs **BEFORE** critical/sensitive communications begin...establishing levels of security due diligence and trust.

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov