Security Control Assessments

Understanding NIST SP 800-53A

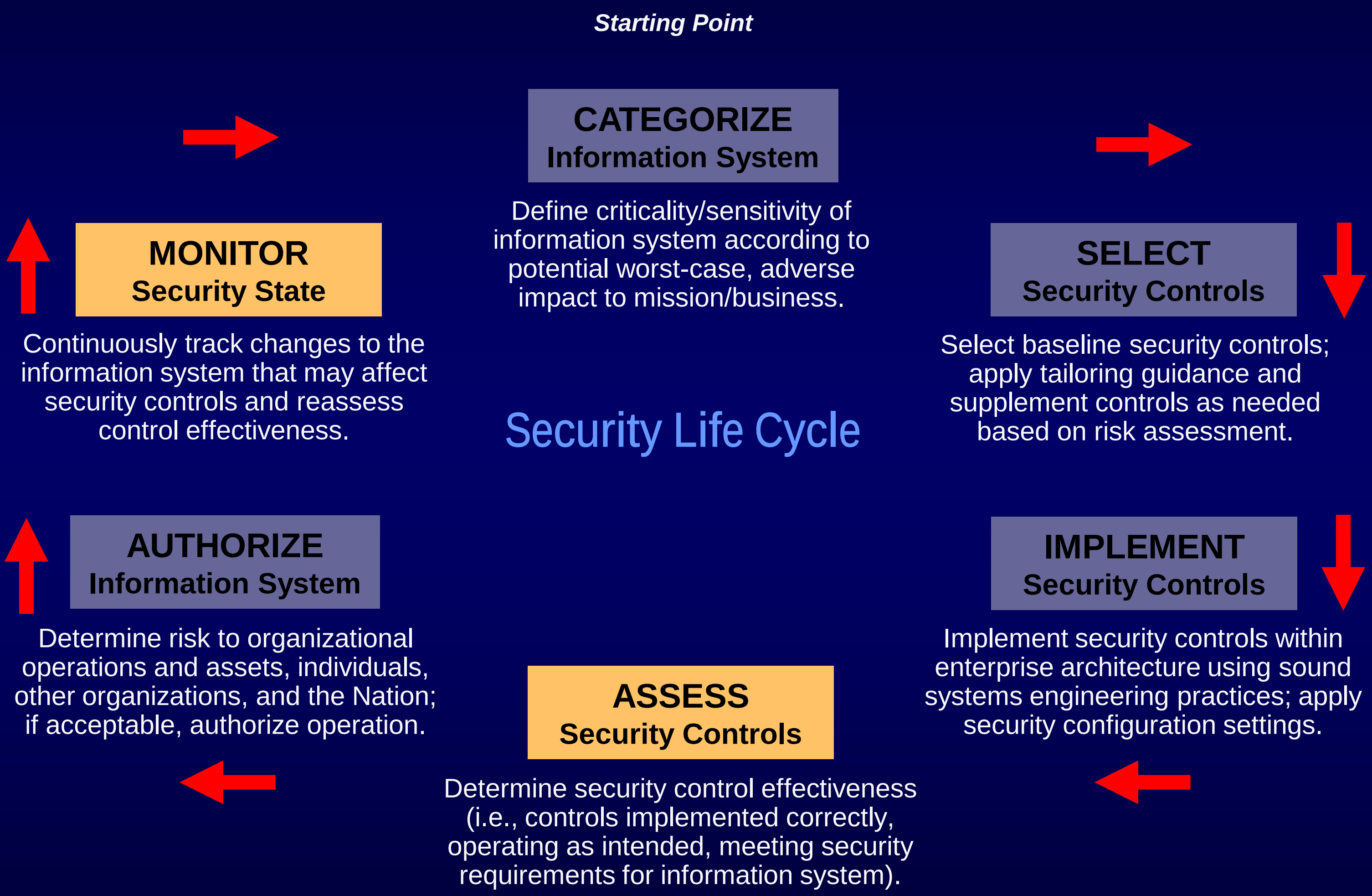
NIST Cryptographic Key Management Workshop

March 5, 2014

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Risk Management Framework



Starting Point

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR
Security State

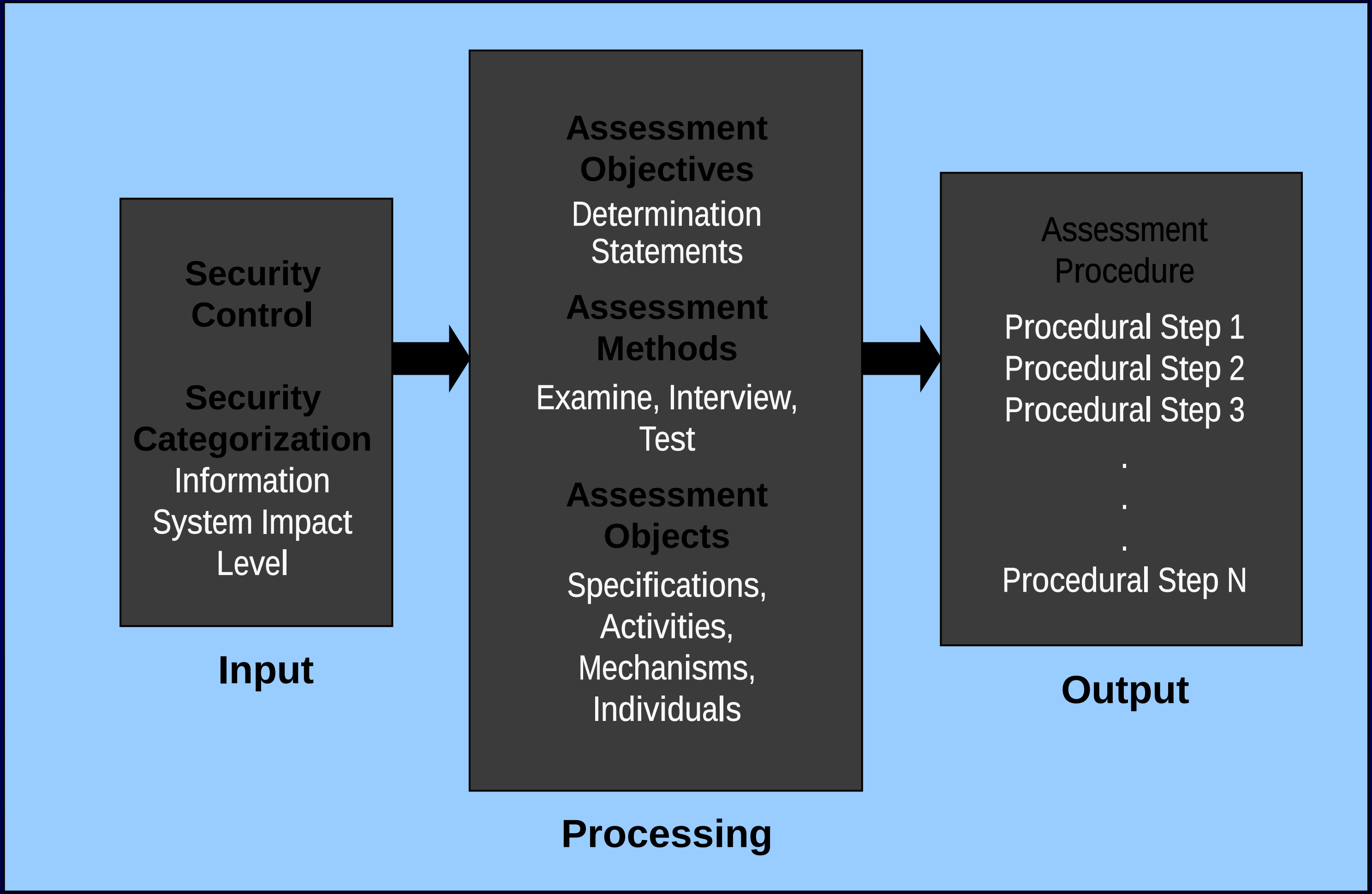
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

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.

Conceptual Assessment Framework



Security Control

Security Categorization

Information System Impact Level

Input

Assessment Objectives

Determination Statements

Assessment Methods

Examine, Interview, Test

Assessment Objects

Specifications, Activities, Mechanisms, Individuals

Processing

Assessment Procedure

Procedural Step 1
Procedural Step 2
Procedural Step 3
.
.
.
Procedural Step N

Output

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 assurance) 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 Procedure Selection

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.

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.
  - Appropriateness of previous analysis.
  - Applicability of the evidence to present information system operating conditions.
  - Amount of time that has transpired since the previous assessments.
  - Degree of independence of the previous assessments.

Assessment Findings

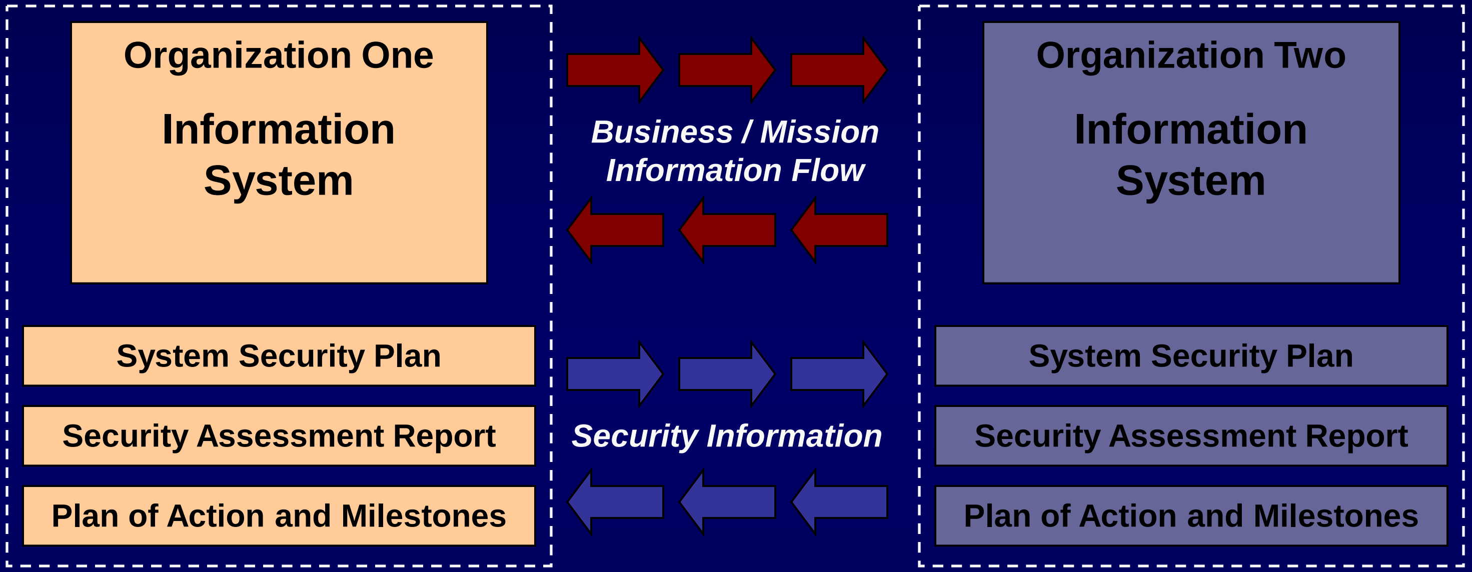
- Are produced for each determination statement in a procedural step executed by an assessor
  - *Satisfied (S)*; or
  - *Other than satisfied (O)*.
- Provide visibility (through objective reporting) into specific weaknesses and deficiencies in the information system.
- Facilitate a disciplined and structured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

Assessment Results

- The security assessment report generates updates to other key documents including:
  - *Security Plan.*
  - *Risk Assessment.*
  - *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.

The Desired End State

Security Visibility Among Business/Mission Partners



Organization One

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Business / Mission Information Flow

Security Information

Organization Two

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

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

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov