NIST Special Publication 800-37

Guide for the Security Certification and Accreditation of Federal Information Systems

An Introductory Tutorial

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Part I
The Fundamentals

National Policy

Office of Management and Budget Circular A-130, *Management of Federal Information Resources* requires federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Authorize system processing prior to operations and periodically, thereafter

Security Controls

- The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

  -- [FIPS Publication 199]

Key Questions

- What security controls are needed to adequately protect an information system that supports the operations and assets of the organization?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- To what extent are the security controls implemented correctly, operating as intended, and producing the desired outcome with respect to meeting information security requirements?

Certification and Accreditation

FISMA and OMB Requirements

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls)
- Publication status:
  - ✓ NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - ✓ Final Publication: May 2004

Purpose and Applicability

Special Publication 800-37

- Provides guidelines for certifying and accrediting information systems supporting the executive agencies of the federal government
- Applies to all federal information systems other than those systems designated as national security systems as defined in FISMA
- Replaces Federal Information Processing Standards (FIPS) Publication 102

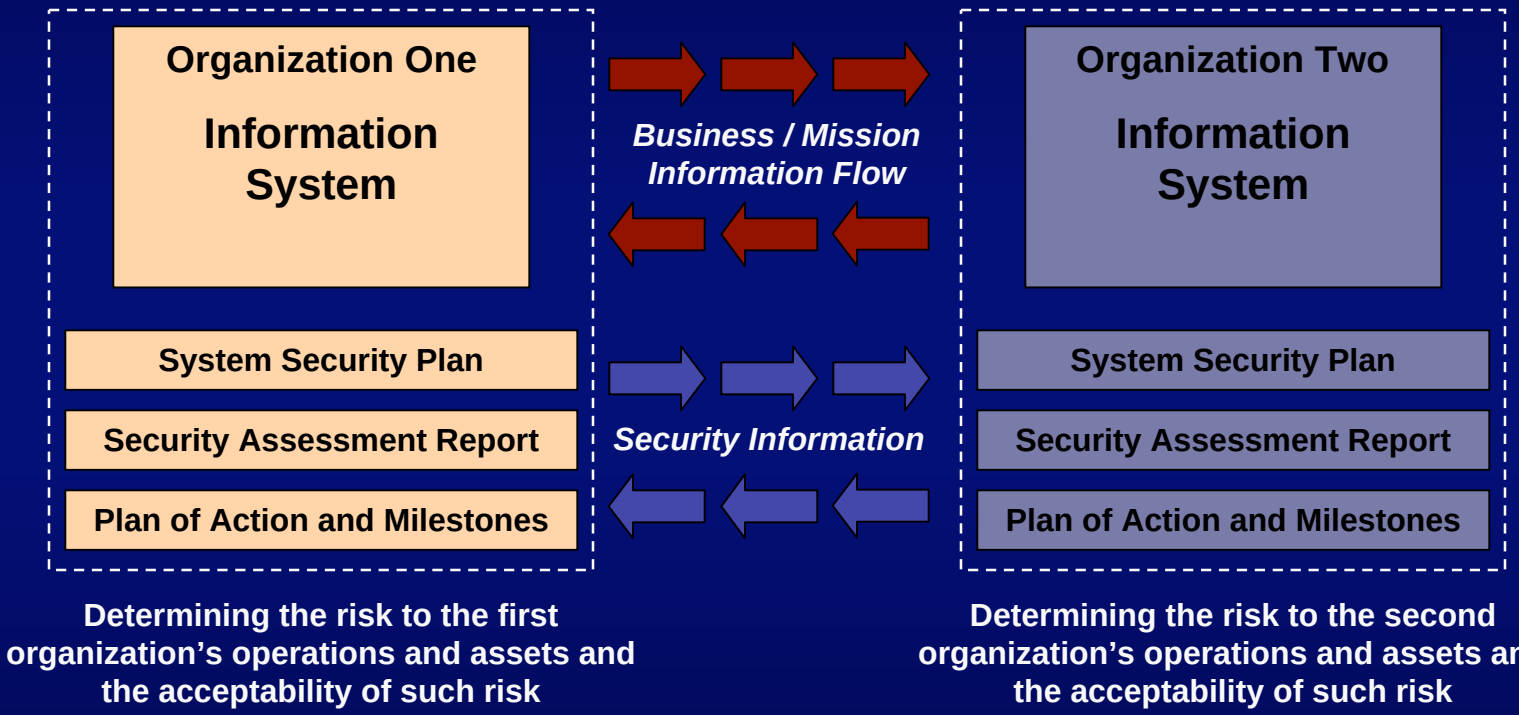
Significant Benefits

Special Publication 800-37

- Helping to achieve more secure information systems within the federal government by:
  - Enabling more consistent, comparable, and repeatable assessments of security controls in federal information systems
  - Promoting a better understanding of agency-related mission risks resulting from the operation of information systems
  - Creating more complete, reliable, and trustworthy information for authorizing officials—facilitating more informed accreditation decisions

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.

Security Accreditation

*O*fficial management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed upon set of security controls.

Security Certification

Comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Key Roles

- Authorizing Official
- Authorizing Official Designated Representative
- Chief Information Officer
- Senior Agency Information Security Officer
- Information System Owner
- Information System Security Officer
- Certification Agent
- User Representatives

Authorizing Official

- Reviews and approves the security categorizations of information systems
- Reviews and approves system security plans
- Determines agency-level risk from information generated during the security certification
- Makes accreditation decisions and signs associated transmittal letters for accreditation packages (authorizing official only)
- Reviews security status reports from continuous monitoring operations; initiates reaccreditation actions

Designated Representative

- Selected by the authorizing official to coordinate and carry out the necessary activities required during the security certification and accreditation process
- Empowered to make certain decisions with regard to the:
  - ✓ Planning and resourcing of the security certification and accreditation activities
  - ✓ Acceptance of the system security plan
  - ✓ Determination of risk to agency operations, assets, and individuals
- Prepares accreditation decision letter
- Obtains authorizing official's signature on the accreditation decision letter and transmits accreditation package to appropriate agency officials

Information System Owner

- Procures, develops, integrates, modifies, operates or maintains an information system
- Prepares system security plan and conducts risk assessment
- Informs agency officials of the need for certification and accreditation; ensures appropriate resources are available
- Provides necessary system-related documentation to the certification agent
- Prepares plan of action and milestones to reduce or eliminate vulnerabilities in the information system
- Assembles final accreditation package and submits to authorizing official

Certification Agent

- Provides an independent assessment of the system security plan
- Assesses the security controls in the information system to determine the extent to which the controls are:
  - ✓ Implemented correctly;
  - ✓ Operating as intended; and
  - ✓ Producing the desired outcome with respect to meeting the security requirements of the system
- Provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system

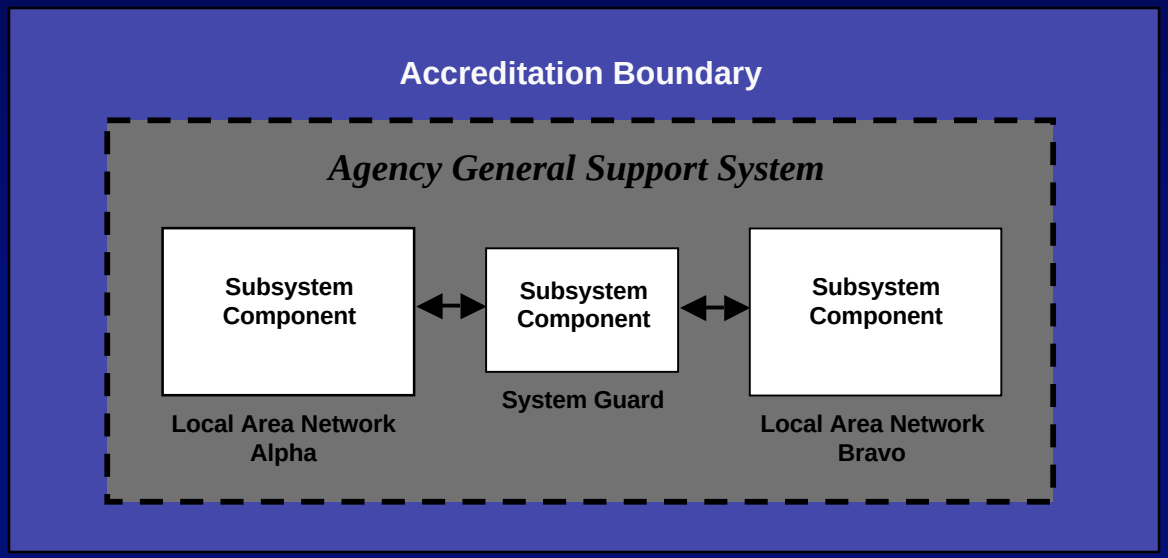
Accreditation Boundaries

- Uniquely assigning information resources to an information system defines the security accreditation boundary for that system
- Agencies have great flexibility in determining what constitutes an information system and the resulting accreditation boundary that is associated with that system

Accreditation Boundaries

- If a set of information resources is identified as an information system, the resources should generally be under the same direct management control
- Consider if the information resources being identified as an information system—
  - Have the same function or mission objective and essentially the same operating characteristics and security needs
  - Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments)

Large and Complex Systems



- System security plan reflects information system decomposition with adequate security controls assigned to each subsystem component
- Security assessment methods and procedures tailored for the security controls in each subsystem component and for the combined system-level controls
- Security certification performed on each subsystem component and on system-level controls not covered by subsystem certifications
- Security accreditation performed on the information system as a whole

Accreditation Decisions

- Authorization To Operate
- Interim Authorization To Operate
- Denial of Authorization to Operate

Accreditation Package

- System security plan
- Security assessment report
- Plan of action and milestones

System Security Plan

- Prepared by the information system owner
- Provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements
- Contains (either as supporting appendices or as references) other key security-related documents for the information system (e.g., risk assessment, contingency plan, incident response plan, system interconnection agreements)

Security Assessment Report

- Prepared by the certification agent
- Provides the results of assessing the security controls in the information system to determine the extent to which the controls are:
  - ✓ Implemented correctly
  - ✓ Operating as intended
  - ✓ Producing the desired outcome with respect to meeting the system security requirements
- Contains a list of recommended corrective actions

Plan of Action and Milestones

- Prepared by the system owner
- Reports progress made on current outstanding items listed in the plan
- Addresses vulnerabilities in the information system discovered during certification, security impact analysis, or security control monitoring
- Describes how the information system owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept vulnerabilities)

Accreditation Decision Letter

- Constructed from information provided by the information system owner in the accreditation package
- Consists of:
  - Accreditation decision
  - Supporting rationale for the decision
  - Specific terms and conditions imposed on the system owner

➢ The contents of security certification and accreditation-related documentation (especially information dealing with system vulnerabilities) should be marked and protected appropriately in accordance with agency policy.

Part II
The Process

The Process

- Initiation Phase
- Security Certification Phase
- Security Accreditation Phase
- Continuous Monitoring Phase

Initiation Phase

Major Tasks and Subtasks

- Task 1: Preparation
  - Subtask 1.1: Information System Description
  - Subtask 1.2: Security Categorization
  - Subtask 1.3: Threat Identification
  - Subtask 1.4: Vulnerability Identification
  - Subtask 1.5: Security Control Identification
  - Subtask 1.6: Initial Risk Determination
- Task 2: Notification and Resource Identification
  - Subtask 2.1: Notification
  - Subtask 2.2: Planning and Resources

Initiation Phase

Major Tasks and Subtasks

- Task 3: System Security Plan Analysis, Update, and Acceptance
  - Subtask 3.1: Security Categorization Review
  - Subtask 3.2: System Security Plan Analysis
  - Subtask 3.3: System Security Plan Update
  - Subtask 3.4: System Security Plan Acceptance

Security Certification Phase

Major Tasks and Subtasks

- Task 4: Security Control Assessment
  - Subtask 4.1: Documentation and Supporting Materials
  - Subtask 4.2: Methods and Procedures
  - Subtask 4.3: Security Assessment
  - Subtask 4.4: Security Assessment Report
- Task 5: Security Certification Documentation
  - Subtask 5.1: Findings and Recommendations
  - Subtask 5.2: System Security Plan Update
  - Subtask 5.3: Plan of Action and Milestones Preparation
  - Subtask 5.4: Accreditation Package Assembly

Security Accreditation Phase

Major Tasks and Subtasks

- Task 6: Accreditation Decision
  - Subtask 6.1: Final Risk Determination
  - Subtask 6.2: Risk Acceptability
- Task 7: Accreditation Documentation
  - Subtask 7.1: Accreditation Package Transmission
  - Subtask 7.2: System Security Plan Update

Continuous Monitoring Phase

Major Tasks and Subtasks

- Task 8: Configuration Management and Control
  - Subtask 8.1: Documentation of System Changes
  - Subtask 8.2: Security Impact Analysis
- Task 9: Security Control Monitoring
  - Subtask 9.1: Security Control Selection
  - Subtask 9.2: Selected Security Control Assessment
- Task 10: Status Reporting and Documentation
  - Subtask 10.1: System Security Plan Update
  - Subtask 10.2: Plan of Action and Milestones Update
  - Subtask 10.3: Status Reporting

Certification and Accreditation

For Low Impact Information Systems

- Incorporates the use of self-assessment activities
- Reduces the associated level of supporting documentation and paperwork
- Decreases the time spent conducting assessment-related activities
- ➢ Significantly reduces costs to the agency without increasing agency-level risk or sacrificing the overall security of the information system.

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