

NIST Special Publication 800-37

*Guide for the Security Certification and Accreditation
of Federal Information Systems*

An Introductory Tutorial

*Computer Security Division
Information Technology Laboratory*

Agenda

- Introduction
- The Fundamentals
- The Process
- Summary

Part I

Introduction

The Global Threat

- Information security is not just a paperwork drill...there are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation's critical information infrastructure and ultimately threaten our economic and national security...

U.S. Critical Infrastructures

Definition

- “...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.”

-- USA Patriot Act (P.L. 107-56)

U.S. Critical Infrastructures

Examples

- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Public Health Systems / Emergency Services
- Information and Telecommunications
- Defense Industry
- Banking and Finance
- Postal and Shipping
- Agriculture / Food / Water
- Chemical

Critical Infrastructure Protection

- The U.S. critical infrastructures are over **90%** owned and operated by the private sector
- Critical infrastructure protection must be a **partnership** between the public and private sectors
- Information security solutions must be broad-based, consensus-driven, and address the ongoing needs of government and industry

FISMA Legislation

The Federal Information Security Management Act of 2002 requires federal agencies to develop, document, and implement an agency wide information security program that includes---

- Periodic testing of the effectiveness of the management, operational, and technical controls of every information system identified in the inventory required under section 3505(c), to be performed with a frequency depending on risk, but no less than annually...

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

Information Security Programs

Question

How do security **certification** and **accreditation** fit into an agency's information security program?

Information Security Programs

Answer

Security **certification** and **accreditation** are important activities that support a risk management process and are an integral part of an agency's overall information security program.

Information Security Program



Links in the Security Chain: Management, Operational, and Technical Controls

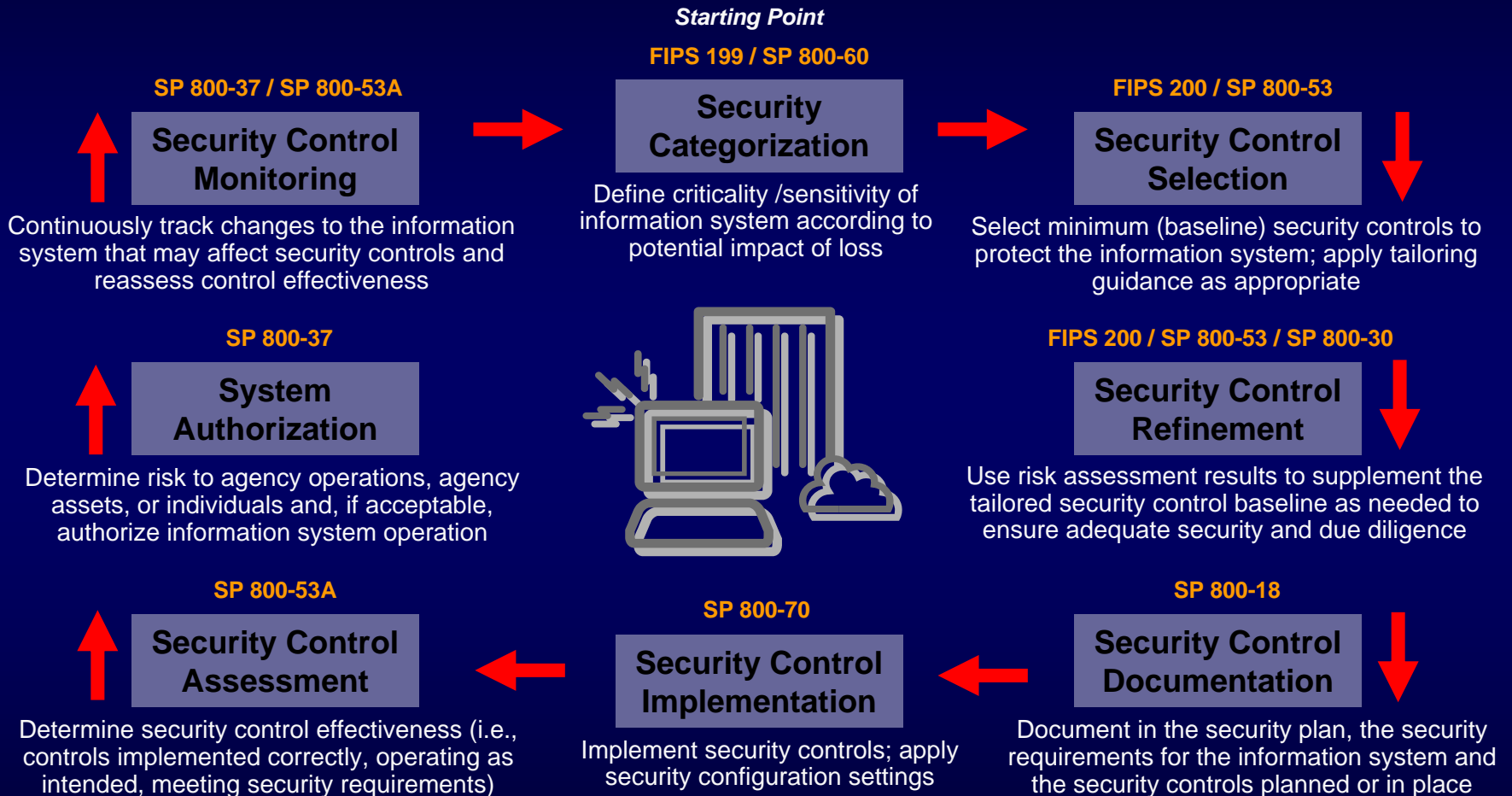
- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Physical security
- ✓ Personnel security
- ✓ Certification, accreditation, and security assessments
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Security configuration settings
- ✓ Anti-viral software
- ✓ Smart cards

Adversaries attack the weakest link...where is yours?

Managing Enterprise Risk

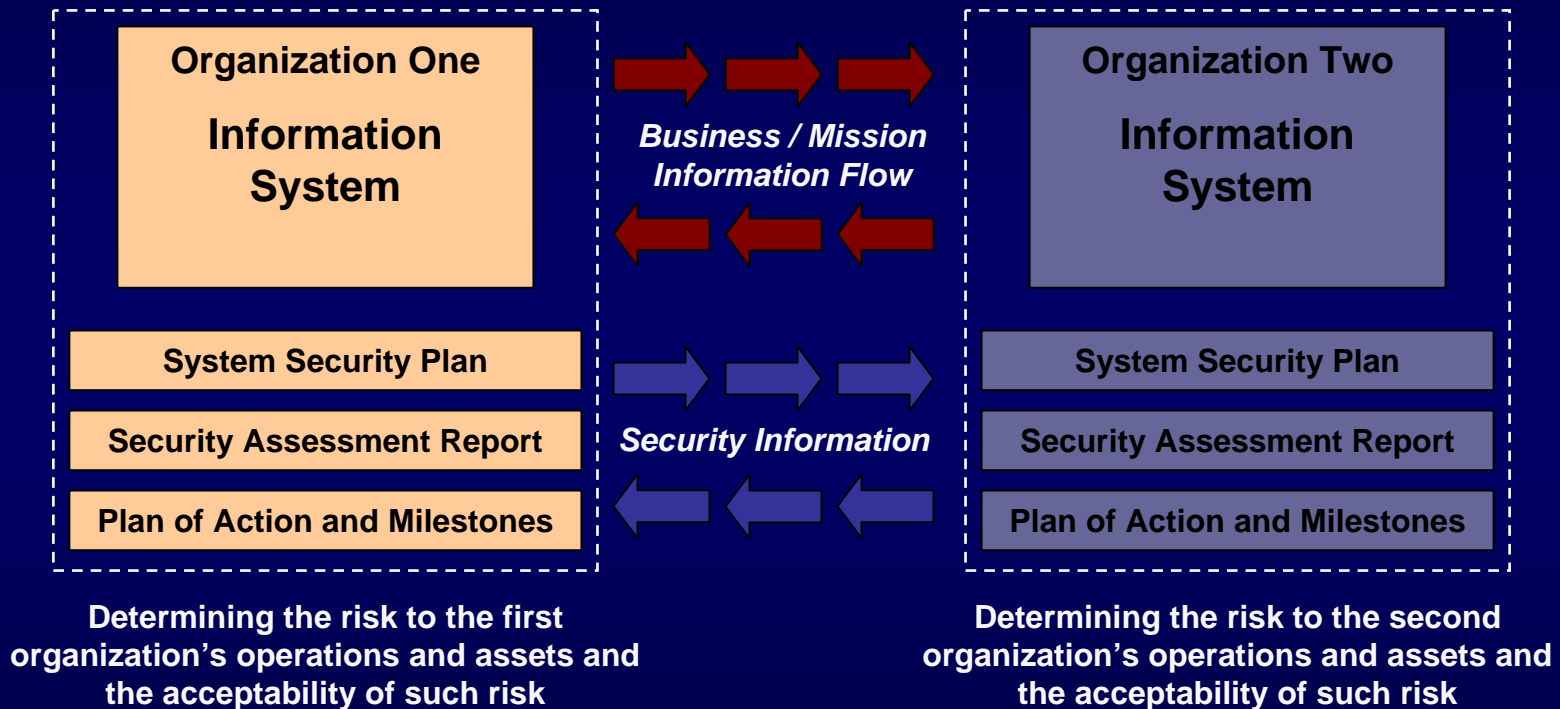
- Key activities in managing **enterprise-level risk**—risk resulting from the operation of an information system:
 - ✓ **Categorize** the information system (criticality/sensitivity)
 - ✓ **Select** and tailor minimum (baseline) security controls
 - ✓ **Supplement** the security controls based on risk assessment
 - ✓ **Document** security controls in system security plan
 - ✓ **Implement** the security controls in the information system
 - ✓ **Assess** the security controls for effectiveness
 - ✓ **Determine** agency-level risk and risk acceptability
 - ✓ **Authorize** information system operation
 - ✓ **Monitor** security controls on a continuous basis

The Risk Framework



The Desired End State

Security Visibility Among Business/Mission Partners



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.

Part II

The Fundamentals

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

Chief Information Officer

- Designates a senior agency information security officer
- Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements
- Trains and oversees personnel with significant responsibilities for information security
- Assists senior agency officials concerning their security responsibilities
- Coordinates with other senior agency officials, reporting annually to the agency head on the effectiveness of the agency information security program

Senior Agency Information Security Officer

- Serves in a position with primary responsibilities and duties related to information security
- Carries out the Chief Information Officer responsibilities under FISMA
- Possesses professional qualifications required to administer information security program functions
- Heads an office with the mission and resources to assist in ensuring agency compliance with FISMA

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

Information System Security Officer

- Serves as principal staff advisor to the system owner on all matters involving the security of the information system
- Manages the security aspects of the information system and, in some cases, oversees the day-to-day security operations of the system
- Assists the system owner in:
 - ✓ Developing and enforcing security policies for the information system
 - ✓ Assembling the security accreditation package
 - ✓ Managing and controlling changes to the information system and assessing the security impacts of those changes

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

User Representatives

- Represent the operational interests and mission needs of the user community
- Identify mission and operational requirements
- Serve as liaisons for the user community throughout the system development life cycle
- Assist in the security certification and accreditation process, when needed

Other Supporting Roles

- Information Owner
- Operations Manager
- Facilities Manager
- System Administrator

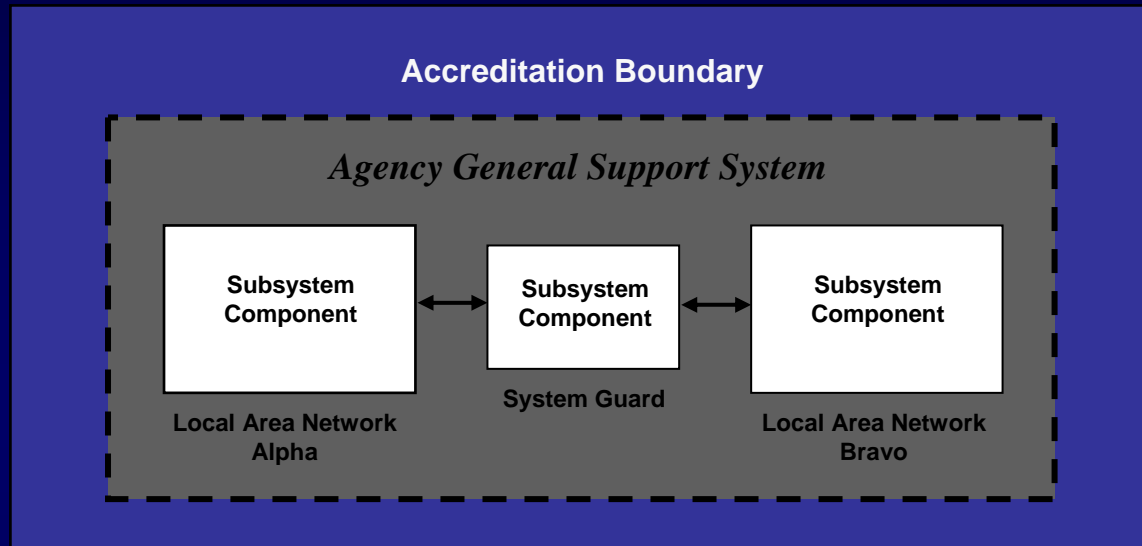
Accreditation Boundaries

- 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

Common Security Controls

- Common security controls are those controls that can be applied to one or more agency information systems and have the following properties:
 - The development, implementation, and assessment of common security controls can be assigned to responsible officials or organizational elements (other than the information system owner)
 - The results from the assessment of the common security controls can be reused in security certifications and accreditations of agency information systems where those controls have been applied

Common Security Controls

- Identification of common security controls is an agency-level activity in collaboration with Chief Information Officer, senior agency information security officer, authorizing officials, information system owners, and information system security officers
- Potential for significant cost savings for the agency in security control development, implementation, and assessment

Common Security Controls

- Common security controls can be applied agency-wide, site-wide, or to common subsystems and assessed accordingly—
For example:

- Contingency planning
- Incident response planning
- Security training and awareness
- Physical and personnel security *
- Common hardware, software, or firmware **

* Related to the concept of site certification in certain communities

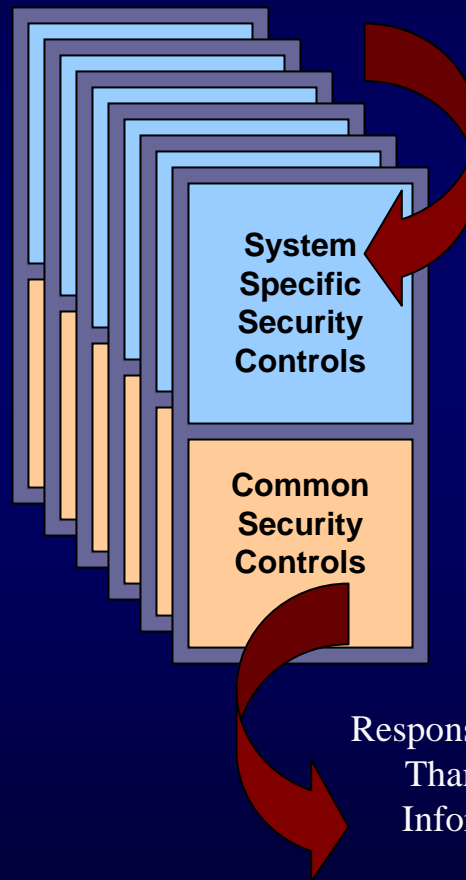
** Related to the concept of type certification in certain communities

Common Security Controls

Responsibility of Information System Owners

Example: Moderate Impact Agency Information Systems

- Maximum re-use of assessment evidence during security certification and accreditation of information systems
- Security assessment reports provided to information system owners to confirm the security status of common security controls
- Assessments of common security controls not repeated; only system specific aspects when necessary



- Common security controls developed, implemented, and assessed one time by designated agency official(s)

- Development and implementation cost amortized across all agency information systems

- Results shared among all information system owners and authorizing officials where common security controls are applied

Responsibility of Designated Agency Official Other Than Information System Owner (e.g., Chief Information Officer, Facilities Manager, etc.)

Accreditation Decisions

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

Authorization to Operate

- Risk to agency operations, agency assets, or individuals is deemed acceptable to the authorizing official
- Information system is accredited without any significant restrictions or limitations on its operation
- Authorizing officials may recommend specific actions be taken to reduce or eliminate identified vulnerabilities, where it is cost effective to do so

Interim Authorization To Operate

- Risk to agency operations, agency assets, or individuals is not deemed acceptable to the authorizing official, but there is an overarching mission necessity to place the information system into operation or continue its operation
- Significant deficiencies in the security controls in the information system but the deficiencies can be addressed in a timely manner
- Acknowledges greater risk to the agency for a limited period of time

Interim Authorization To Operate

- Limited authorization to operate the information system under specific terms and conditions established by the authorizing official
- Information system is *not* accredited during the period of limited authorization to operate
- At the end of the period of limited authorization, the information system should either meet the requirements for being authorized or not be authorized for further operation

Denial of Authorization to Operate

- The residual risk to the agency's operations or assets is deemed unacceptable to the authorizing official
- Information system is not accredited and should not be placed into operation—or for an information system currently in operation, all activity should be halted
- Major deficiencies in the security controls in the information system—corrective actions should be initiated immediately

Accreditation Package

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

Accreditation Package

- Documents the results of the security certification
- Provides the authorizing official with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system
- Uses inputs from the information system security officer and the certification agent

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 III

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.

Part V

Summary

Special Publication 800-37

Intended to promote and facilitate—

- More consistent, comparable, and repeatable assessments of information systems
- More complete and reliable security-related information for authorizing officials
- A better understanding of complex information systems and associated risks and vulnerabilities

The Golden Rules

Building an Effective Enterprise Information Security Program

- Develop an enterprise-wide information security strategy and game plan
- Get corporate “buy in” for the enterprise information security program—effective programs start at the top
- Build information security into the infrastructure of the enterprise
- Establish level of “due diligence” for information security
- Focus initially on mission/business case impacts—bring in threat information only when specific and credible

The Golden Rules

Building an Effective Enterprise Information Security Program

- Create a balanced information security program with management, operational, and technical security controls
- Employ a solid foundation of security controls first, then build on that foundation guided by an assessment of risk
- Avoid complicated and expensive risk assessments that rely on flawed assumptions or unverifiable data
- Harden the target; place multiple barriers between the adversary and enterprise information systems
- Be a good consumer—beware of vendors trying to sell “single point solutions” for enterprise security problems

The Golden Rules

Building an Effective Enterprise Information Security Program

- Don't be overwhelmed with the enormity or complexity of the information security problem—take one step at a time and build on small successes
- Don't tolerate indifference to enterprise information security problems

And finally...

- Manage enterprise risk—don't try to avoid it!

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