FISMA Implementation Project

Protecting the Nation's Critical Information Infrastructure

An Overview

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Agenda

- Introduction
- Managing Enterprise Risk
- Special Publication 800-53
- Cost-effective Implementation
- Summary

Part I

Introduction

Today’s Climate

- Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- The complexity of today’s systems and networks presents great security challenges for both producers and consumers of information technology

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…

The Advantage of the Offense

- Powerful attack tools now available over the Internet to anyone who wants them
- Powerful, affordable computing platforms to launch sophisticated attacks now available to the masses
- Little skill or sophistication required to initiate extremely harmful attacks

Result: The sophistication of the attack is growing, but the sophistication of the attacker is not.

Key Security Challenges

- Adequately protecting enterprise information systems within constrained budgets
- Changing the current culture of:

  "Connect first…ask security questions later"

- Bringing standards to:
  - ✓ Information system security control selection and specification
  - ✓ Methods and procedures employed to assess the correctness and effectiveness of those controls

Legislative and Policy Drivers

- Public Law 107-347 (Title III)
  Federal Information Security Management Act of 2002
- Homeland Security Presidential Directive #7
  Critical Infrastructure Identification, Prioritization, and Protection
- OMB Circular A-130 (Appendix III)
  Security of Federal Automated Information Resources

FISMA Legislation

Overview

"Each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

-- Federal Information Security Management Act of 2002

FISMA Tasks for NIST

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category

FISMA Implementation Project

- Phase I: To develop standards and guidelines for:
  - Categorizing Federal information and information systems
  - Selecting minimum security controls for Federal information systems
  - Assessing the security controls in Federal information systems

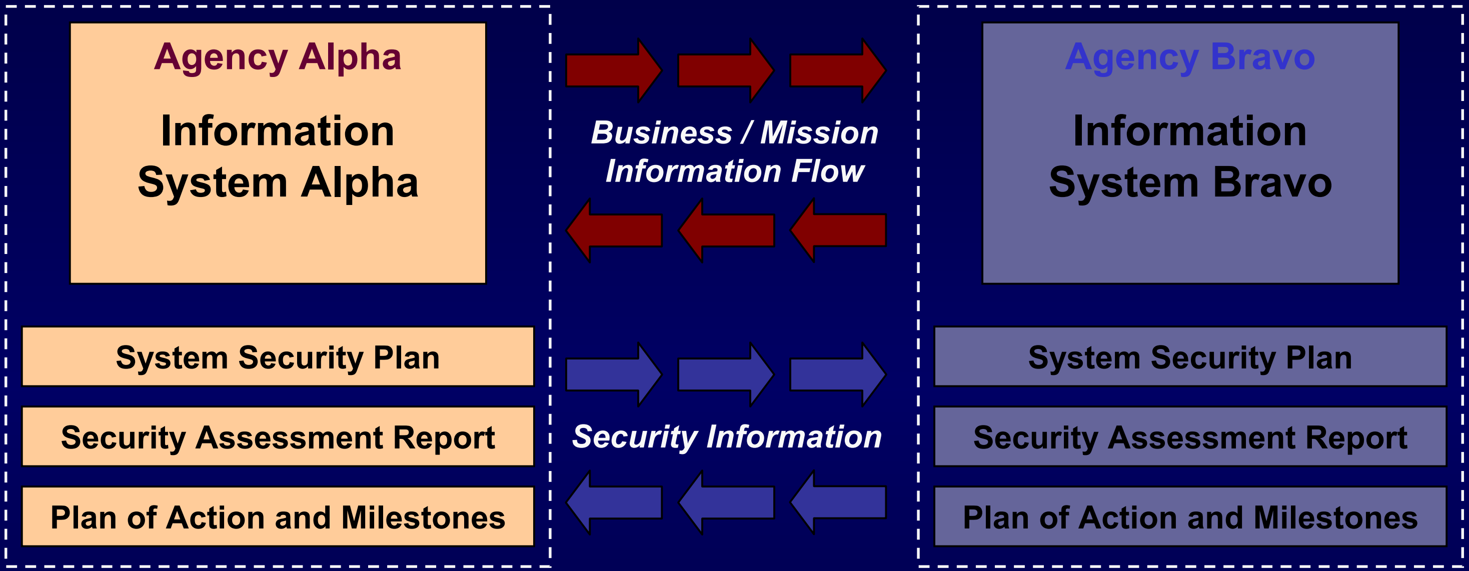
Phase II: To create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the NIST standards and guidelines

Significant Benefits

- More consistent and comparable specifications of security controls for information systems
- More consistent, comparable, and repeatable system-level 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
- Greater availability of competent security assessment services

The Desired End State

Security Visibility Among Business/Mission Partners



Agency Alpha

Information System Alpha

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Business / Mission Information Flow

Security Information

Agency Bravo

Information System Bravo

System Security Plan

Security Assessment Report

Plan of Action and Milestones

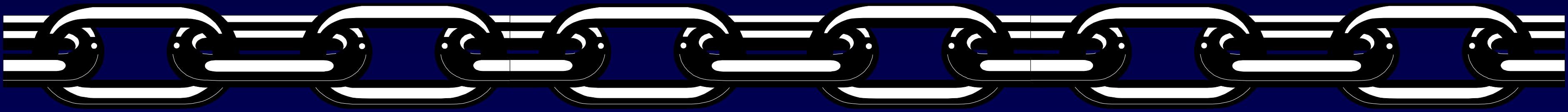
Determination of risk to Agency Alpha's operations, agency assets, or individuals and acceptability of such risk

Determination of risk to Agency Bravo's operations, agency assets, or individuals and acceptability of such risk

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

Part II
Managing Enterprise Risk

The Security Chain



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

- ✓ Risk management
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Physical security
- ✓ Personnel security
- ✓ Security Assessments
- ✓ Security Accreditation

- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Anti-viral software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

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]

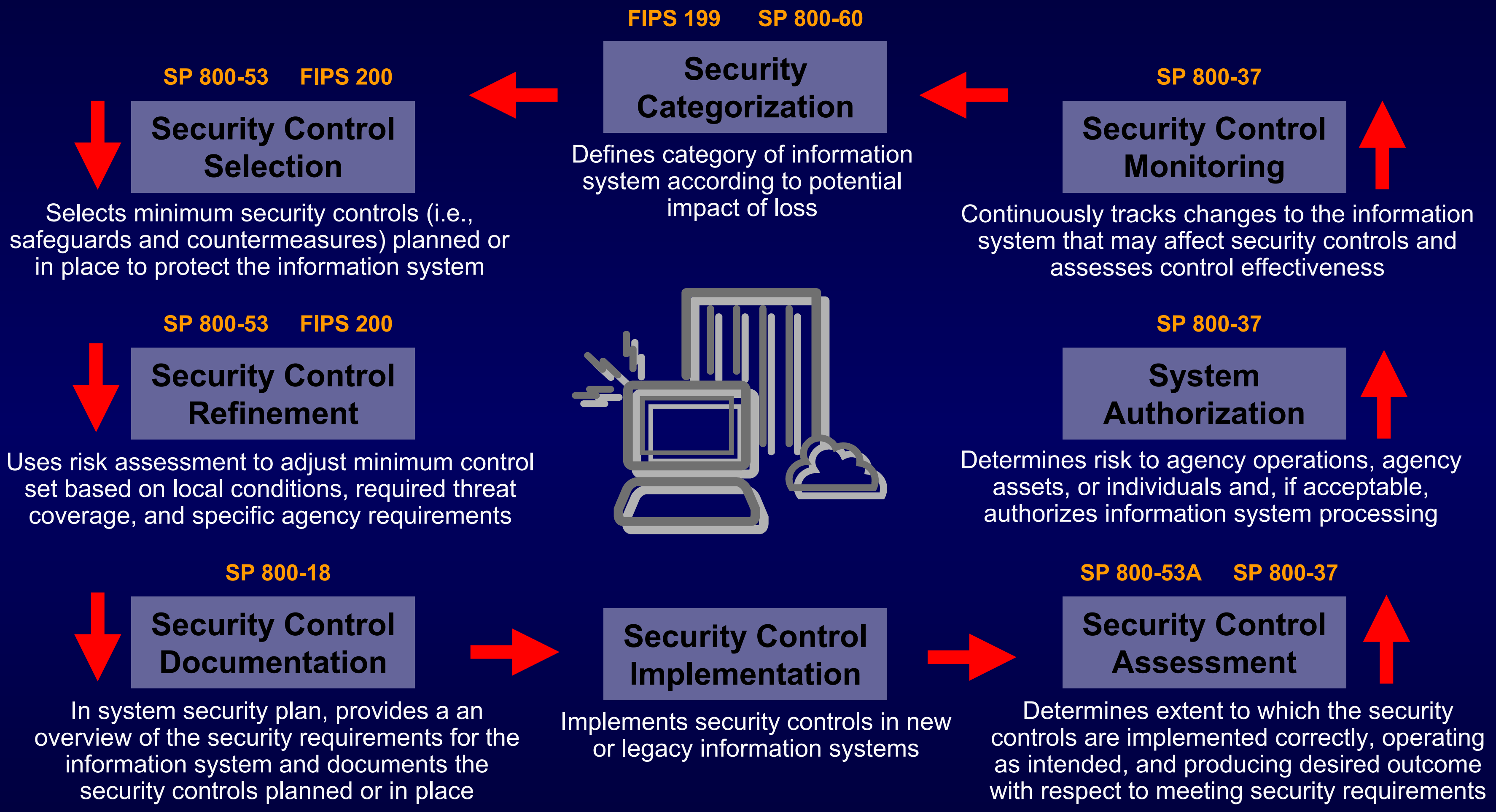
Key Questions

- 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?

Managing Enterprise Risk

- Key activities in managing risk to agency operations, agency assets, or individuals resulting from the operation of an information system—
  - ✓ **Categorize** the information system
  - ✓ **Select** set of minimum (baseline) security controls
  - ✓ **Refine** the security control set based on risk assessment
  - ✓ **Document** agreed upon security controls in security plan
  - ✓ **Implement** the security controls in the information system
  - ✓ **Assess** the security controls
  - ✓ **Determine** agency-level risk and risk acceptability
  - ✓ **Authorize** information system operation
  - ✓ **Monitor** security controls on a continuous basis

Risk Management Framework



FIPS 199 SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-53 FIPS 200

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

Security Control Implementation

Implements security controls in new or legacy information systems

SP 800-53A SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-37

Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

Categorization Standards

NIST FISMA Requirement #1

- Develop standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
  - ✓ Final Publication: December 2003
  - ✓ Signed by Secretary of Commerce: February 2004

Mapping Guidelines

NIST FISMA Requirement #2

- Develop guidelines recommending the types of information and information systems to be included in each category described in FIPS Publication 199
- Publication status:
  - ✓ NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"
  - ✓ Initial Public Draft: December 2003

Minimum Security Requirements

NIST FISMA Requirement #3

- Develop minimum information security requirements (i.e., management, operational, and technical security controls) for information and information systems in each such category—
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*
  - ✓ Final Publication: December 2005

* NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems", (Initial public draft, October 2003), will provide interim guidance until completion and adoption of FIPS Publication 200.

Certification and Accreditation

Supporting FISMA 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: April 2004

Certification and Accreditation

Supporting FISMA Requirements

- Provides standardized assessment methods and procedures to determine the extent to which the security controls in an information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting system security requirements
- Publication status:
  - ✓ NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems"
  - ✓ Initial Public Draft: Summer 2004

Part III

Special Publication 800-53

Special Publication 800-53

The purpose of SP 800-53 is to provide—

- Guidance on how to use a FIPS Publication 199 security categorization to identify minimum security controls (baseline) for an information system
- Minimum (baseline) sets of security controls for low, moderate, and high impact information systems
- Estimated threat coverage for each baseline
- A catalog of security controls for information systems requiring additional threat coverage

Applicability

- Applicable to all Federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542
- Broadly developed from a technical perspective to complement similar guidelines issued by agencies and offices operating or exercising control over national security systems
- Provides guidance to Federal agencies until the publication of FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*

Special Publication 800-53

- Special Publication 800-53 is ***not*** a tutorial on the security control selection process or a security engineering handbook. An additional guidance document is needed that addresses:
  - Relationship of minimum security controls (baselines) to threat coverage
  - Relationships among basic, enhanced, and strong controls
  - How to select additional security controls from the control catalogue

Document Architecture

- Main Body
- Catalog of Security Controls (complete set)
  - Minimum Security Controls for Low Impact Systems (subset of controls from catalog)
  - Minimum Security Controls for Moderate Impact Systems (subset of controls from catalog)
  - Minimum Security Controls for High Impact Systems (subset of controls from catalog)
- Estimated Threat Coverage

Security Categorization

Potential Impact

Security Objective

FIPS Publication 199	**Low**	**Moderate**	**High**
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Categorization

Example: Law Enforcement Witness Protection Information System

Guidance for Mapping Types of Information and Information Systems to FIPS Publication 199 Security Categories

SP 800-60

FIPS Publication 199	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Categorization

Example: Law Enforcement Witness Protection Information System

Guidance for Mapping Types of Information and Information Systems to FIPS Publication 199 Security Categories

SP 800-60

FIPS Publication 199	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or** [illegible] **ic** adverse eff[illegible] nizational ope[illegible] ganizational asse[illegible] iduals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The [illegible] lability could be ex[illegible] ave a **severe or cat**[illegible] dverse effect o[illegible] ional operation[illegible] tional assets, or in[illegible]

Minimum Security Controls for High Impact Systems

Why High Water Mark

- Strong dependencies among security objectives of confidentiality, integrity, and availability
- In general, the impact values for all security objectives must be commensurate—a lowering of an impact value for *one* security objective might affect *all* other security objectives
  - Example: A lowering of the impact value for confidentiality and the corresponding employment of weaker security controls may result in a breach of security due to an unauthorized disclosure of system password tables—thus, causing a subsequent integrity loss and denial of service…

Minimum Security Controls

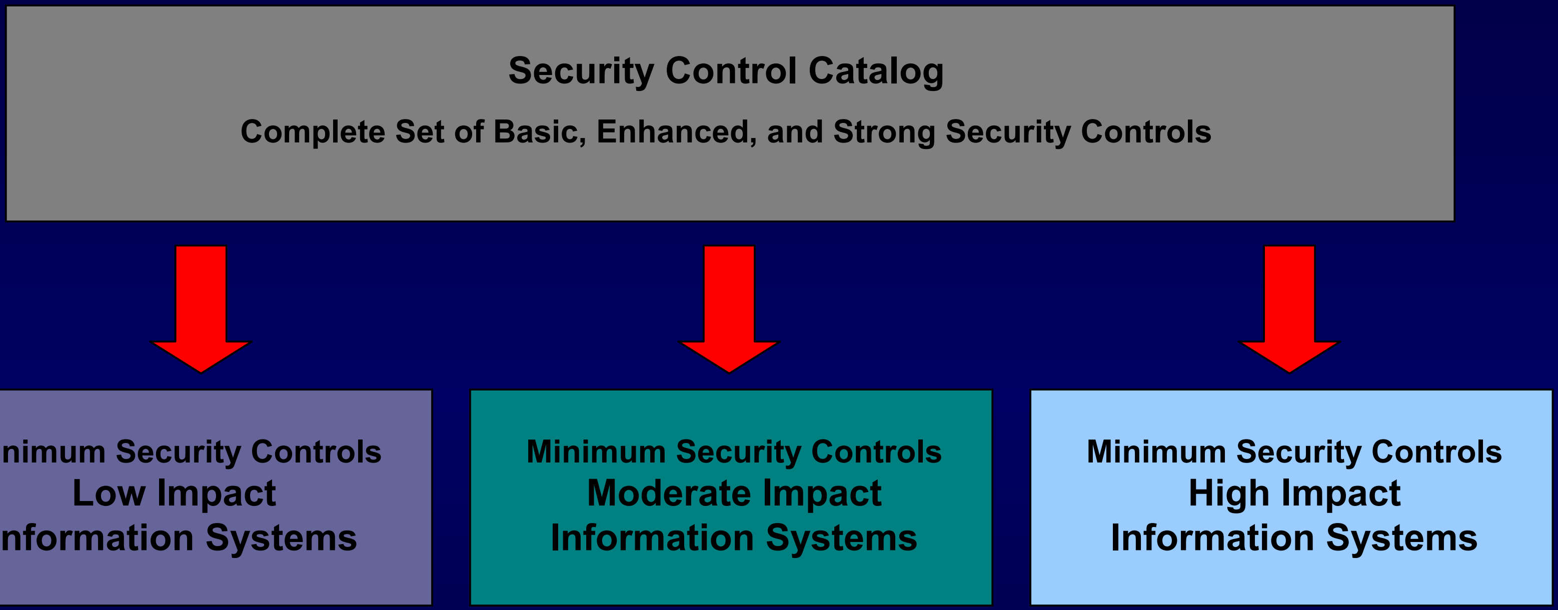
- Minimum security controls and associated threat coverage in each of the designated baselines:
  - Provide a *starting point* for organizations and communities of interest in their security control selection process
  - Are used in the within the context of the agency's ongoing *risk management process*

Terminology

- Security control strength or goodness rating defined in the control catalog as:
  - **Basic**
  - **Enhanced**
  - **Strong**
- Appropriate security controls from the catalog are selected to populate the sets of minimum security controls (baselines) for:
  - **Low** impact information systems
  - **Moderate** impact information systems
  - **High** impact information systems
- No direct correlation between strength/goodness rating and impact level—select the controls best suited to do the job…

Minimum Security Controls Sets

Baselines Provided by Special Publication 800-53



Security Control Catalog

Complete Set of Basic, Enhanced, and Strong Security Controls

Minimum Security Controls
Low Impact
Information Systems

Minimum Security Controls
Moderate Impact
Information Systems

Minimum Security Controls
High Impact
Information Systems

Baseline #1

Selection of a subset of security controls from the catalog—all ***basic*** level controls

Baseline #2

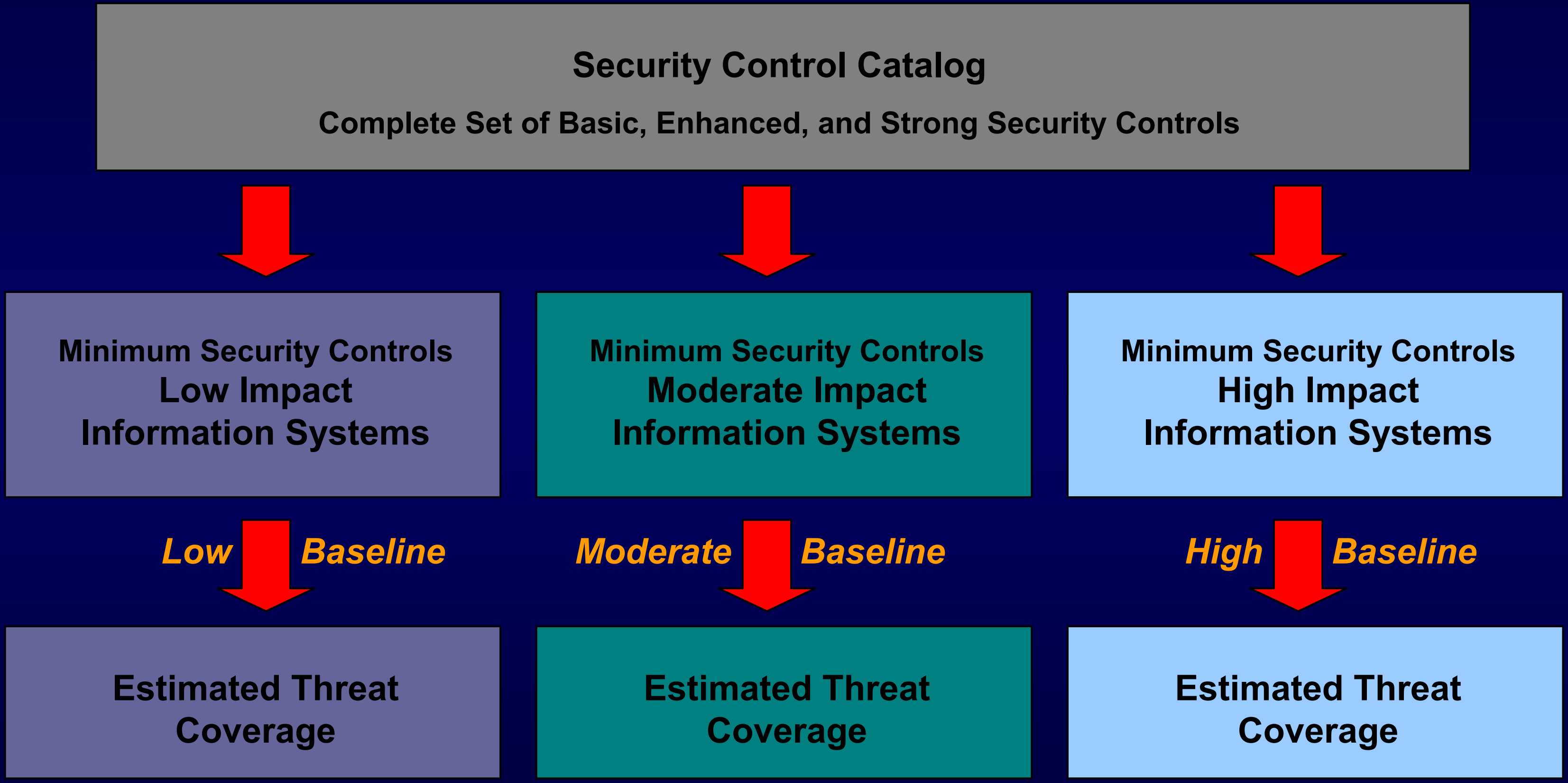
Selection of a subset of security controls from the catalog—combination of ***basic*** and **enhanced** controls

Baseline #3

Selection of a subset of security controls from the catalog—combination of ***basic***, ***enhanced***, and ***strong*** controls

Estimated Threat Coverage

Provided by Special Publication 800-53



Security Control Catalog

Complete Set of Basic, Enhanced, and Strong Security Controls

Minimum Security Controls
Low Impact
Information Systems

Minimum Security Controls
Moderate Impact
Information Systems

Minimum Security Controls
High Impact
Information Systems

Low Baseline

Moderate Baseline

High Baseline

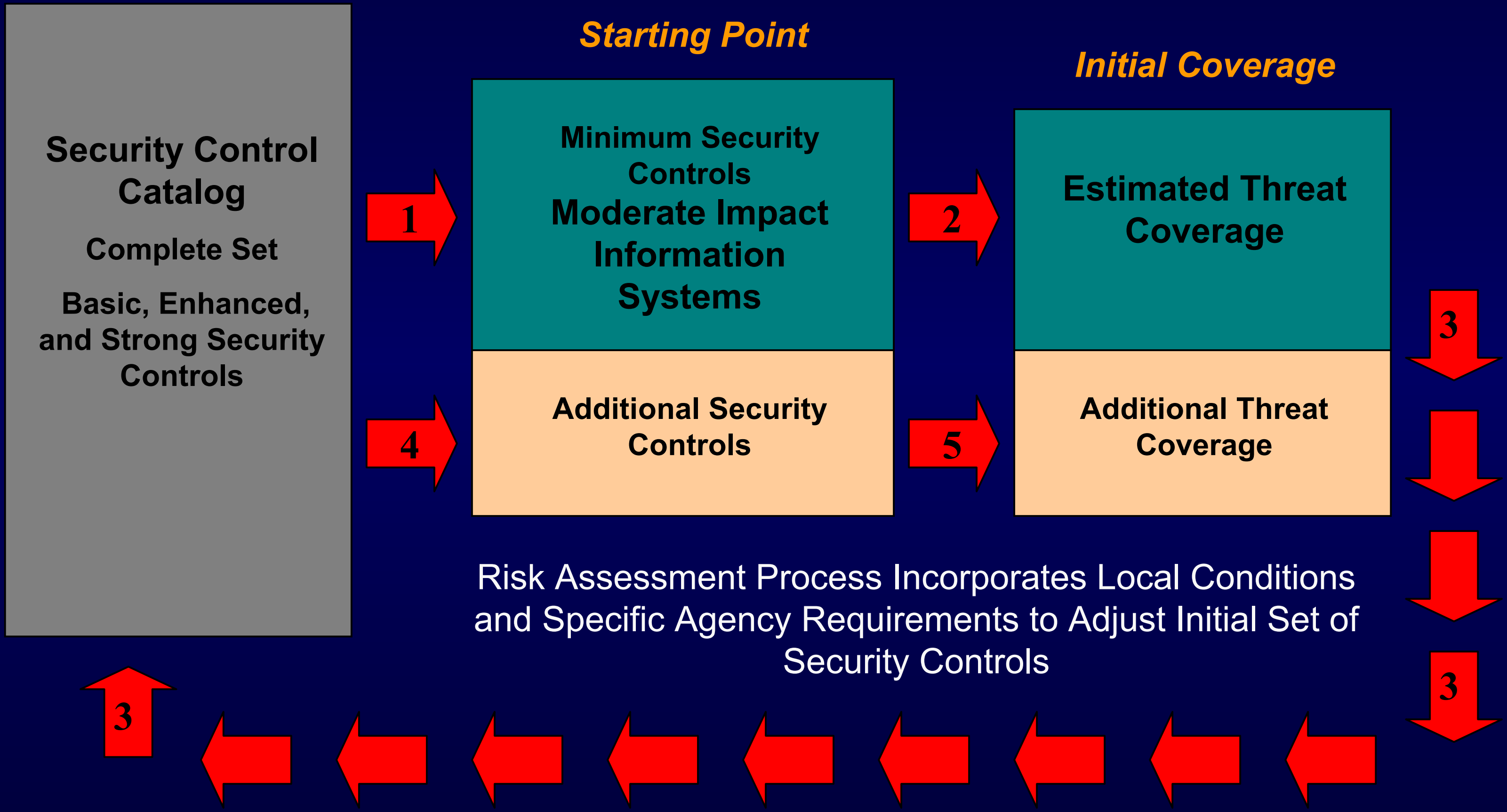
Estimated Threat Coverage

Estimated Threat Coverage

Estimated Threat Coverage

Security Control Refinement

Agency-level Activity Guided by Risk Assessment



Security Control Catalog

Complete Set

Basic, Enhanced, and Strong Security Controls

Starting Point

Minimum Security Controls

Moderate Impact Information Systems

Initial Coverage

Estimated Threat Coverage

Additional Security Controls

Additional Threat Coverage

Risk Assessment Process Incorporates Local Conditions and Specific Agency Requirements to Adjust Initial Set of Security Controls

Tagging of Security Controls

Why aren't security controls partitioned by security objectives (e.g., Confidentiality, Integrity, Availability)?

- In general, it is difficult to assign proper security objectives (i.e., confidentiality, integrity, or availability) to individual security controls
- In many cases, multiple security objectives apply to a single security control
- Availability may be the exception due to the potential for downgrading availability impact values during FIPS 199 security categorizations

Part IV

Cost Effective Implementation

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, authorizing officials, information system owners, system security managers, and 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

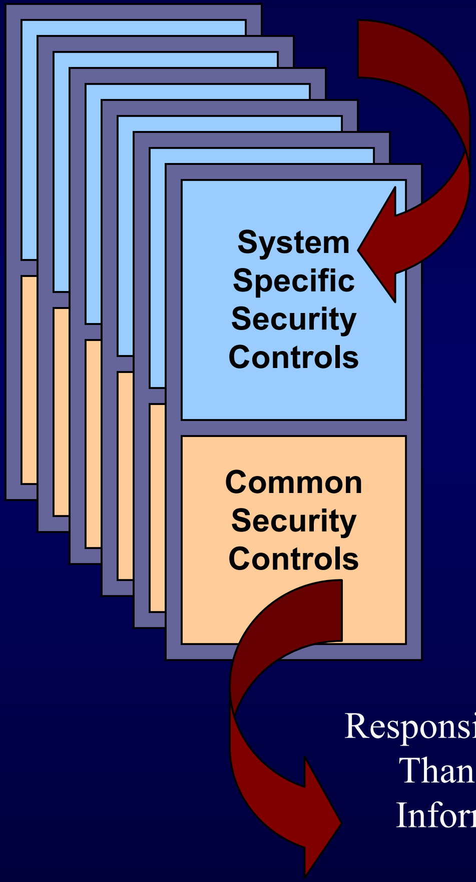
Responsibility of Information System Owners

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.)

Part V
Summary

The Bottom Line

- Standardized security controls facilitate—
  - More consistent, comparable specifications of security controls for information systems
  - Comparability of security plans among business/mission partners
  - A better understanding of the effectiveness of business/mission partner’s security controls and the vulnerabilities in their information systems
  - Greater insights into business/mission partner’s due diligence with regard to security and tolerance for agency-level, mission-related risk

NIST Standards and Guidelines

Are intended to promote and facilitate—

- More consistent, comparable specifications of security controls for information systems
- More consistent, comparable, and repeatable system 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
- Greater availability of competent security assessment services

FISMA Implementation Project

Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- NIST Special Publication 800-37 (C&A)
- NIST Special Publication 800-53 (Security Controls)
- NIST Special Publication 800-53A (Assessment)
- NIST Special Publication 800-59 (National Security)
- NIST Special Publication 800-60 (Category Mapping)
- FIPS Publication 200 (Minimum Security Controls)

Contact Information

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

Project Manager

Dr. Ron Ross
(301) 975-5390
rross@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

Annabelle Lee
(301) 975-2941
annabelle.lee@nist.gov

Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

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

Comments to: sec-cert@nist.gov
World Wide Web: http://csrc.nist.gov/sec-cert