Building More Secure Information Systems

A Strategy for Effectively Applying the Provisions of FISMA

Presented to the FISSEA Conference

March 23, 2005

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The Information Age

- Information systems are an integral part of government and business operations today
- Information systems are changing the way we do business and interact as a society
- Information systems are driving a reengineering of business processes in all sectors including defense, healthcare, manufacturing, financial services, etc.
- Information systems are driving a transition from a paper-based society to a digital society

The Protection Gap

- Information system protection measures have not kept pace with rapidly advancing technologies
- Information security programs have not kept pace with the aggressive deployment of information technologies within enterprises
- Two-tiered approach to security (i.e., national security community vs. everyone else) has left significant parts of the critical infrastructure vulnerable

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

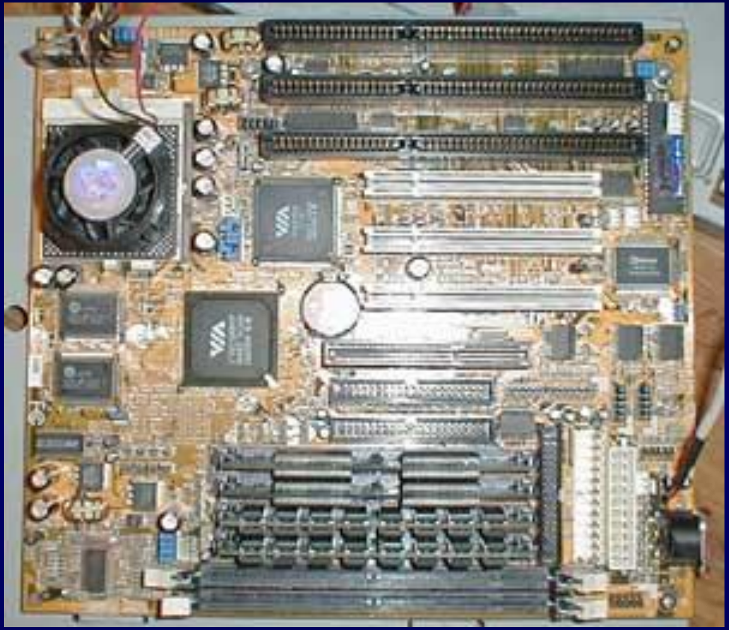
- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Public Health Systems / Emergency Services
- Information and Telecommunications
- Defense Industry
- Banking and Finance
- Postal and Shipping
- Agriculture / Food / Water
- Chemical

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

Threats to Security

Connectivity



Complexity

Key Security Challenges

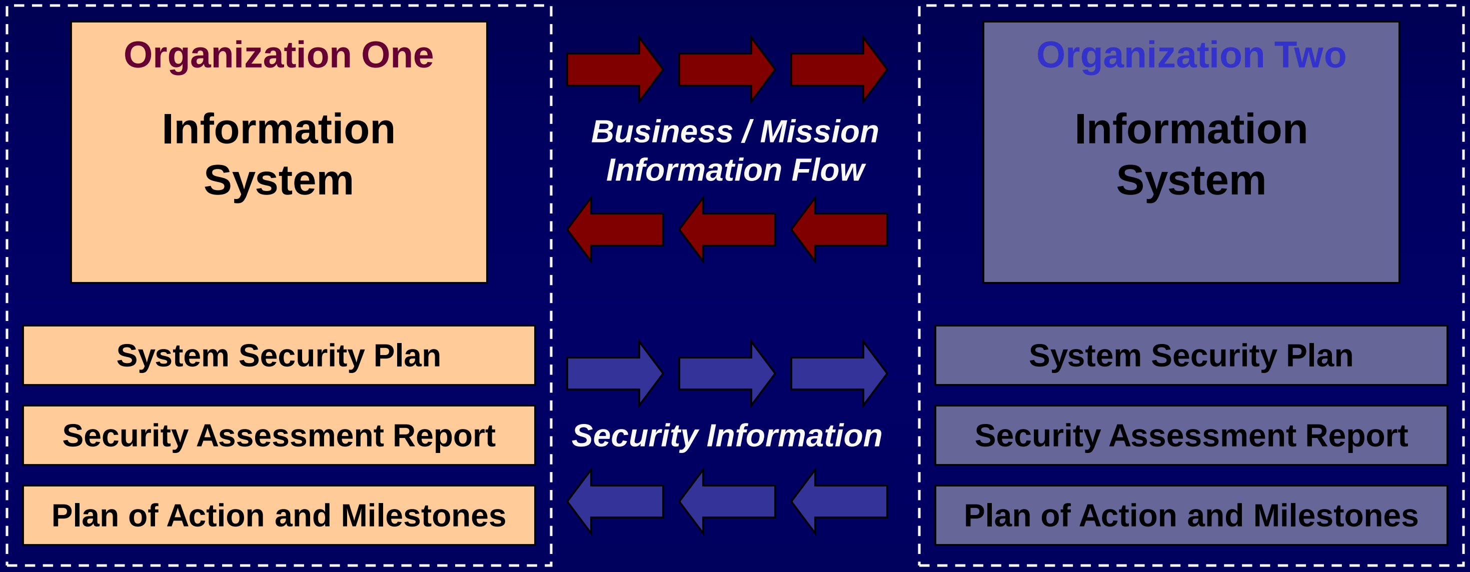
- Adequately protecting enterprise information systems within constrained budgets
- Changing the current culture of:

  "Connect first…ask security questions later"

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

Why Standardization?

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.

Legislative and Policy Drivers

- Public Law 107-347 (Title III)
  Federal Information Security Management Act of 2002
- Public Law 107-305
  Cyber Security Research and Development 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 Implementation Project

Current and Future Activities

- Phase I: Development of FISMA-related security standards and guidelines
  Status: Currently underway and nearing completion

- Phase II: Development of accreditation program for security service providers
  Status: Projected start in 2006; partially funded

- Phase III: Development of validation program for information security tools
  Status: No projected start date; currently not funded

FISMA Implementation Project

Standards and Guidelines

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

Categorization Standards

FISMA Requirement

- 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*

* FIPS Publication 199 was signed by the Secretary of Commerce in February 2004.

Security Categorization

Example: An Enterprise 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: An Enterprise 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 exp [illegible] ave a **severe or cata** [illegible] dverse effect o [illegible] ional operation [illegible] ional assets, or in [illegible]

Minimum Security Controls for High Impact Systems

Mapping Guidelines

FISMA Requirement

- Develop guidelines recommending the types of information and information systems to be included in each category
- Publication status:
  - ✓ NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"
  - ✓ Final Publication: June 2004

Minimum Security Requirements

FISMA Requirement

- Develop minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category

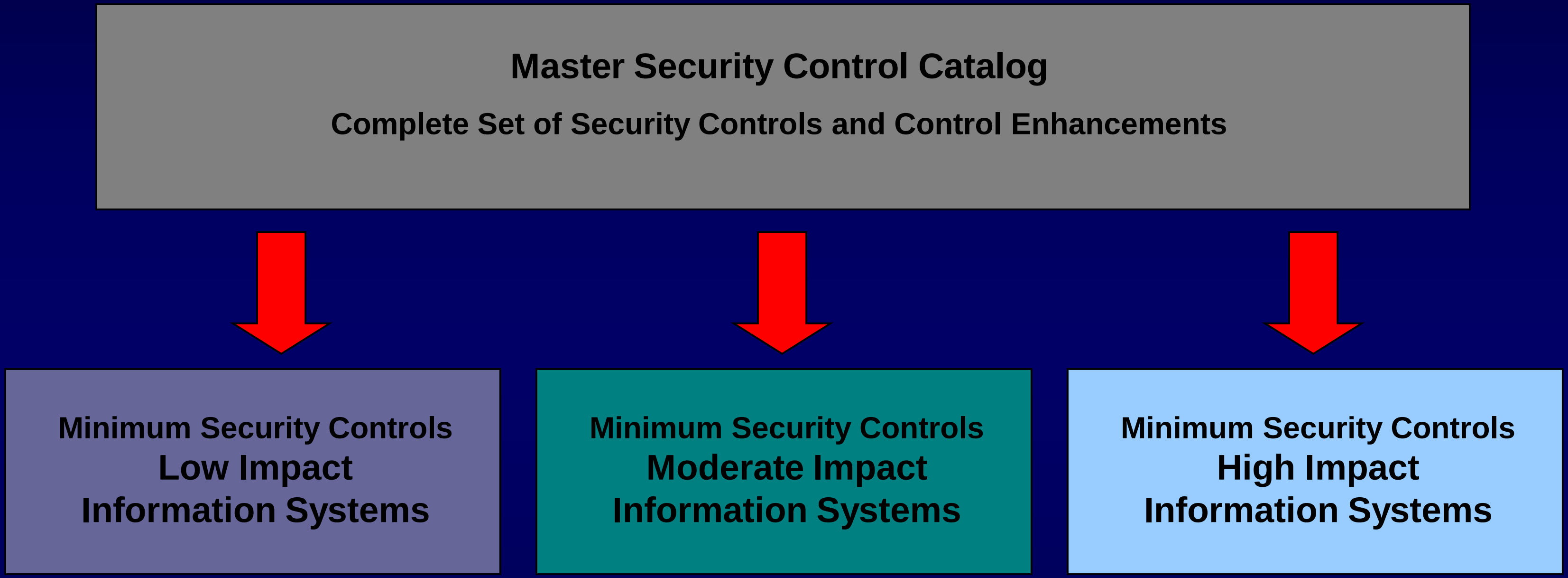
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*
  - ✓ Final Publication: December 2005

* NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" (Final publication February 2005) will provide interim guidance until completion and adoption of FIPS Publication 200.

Minimum Security Controls

- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
  - Provide a ***starting point*** for organizations in their security control selection process
  - Are used in conjunction with ***scoping guidance*** that allows the baseline controls to be tailored for specific operational environments
  - Support the organization's ***risk management process***

Security Control Baselines



Master Security Control Catalog

Complete Set of Security Controls and Control Enhancements

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 master catalog—consisting of ***basic*** level controls

Baseline #2

Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Baseline #3

Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Security Control Assessment

FISMA Requirement

- 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 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems”
  - ✓ Initial Public Draft: Spring 2005

Certification and Accreditation

Supporting FISMA Requirement

- 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

Security Checklists

CSRDA Requirement

- Develop and disseminate security configuration checklists and option selections that minimize the security risks associated with commercial information technology products that are, or are likely to become, widely used within federal information systems
- Publication status:
  - ✓ NIST Special Publication 800-70, "The NIST Security Configuration Checklists Program"
  - ✓ Initial Public Draft: August 2004

Putting It All Together

Question

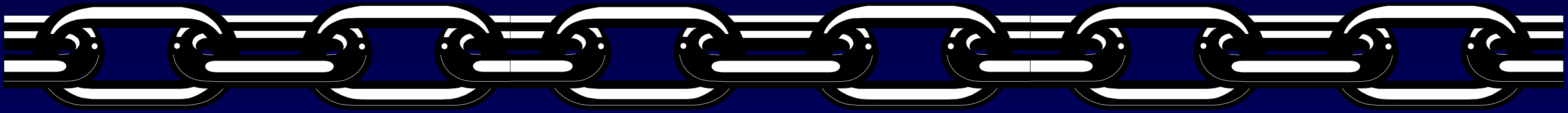
How does the family of FISMA-related publications fit into an organization’s information security program?

An Integrated Approach

Answer

NIST publications in the FISMA-related series provide security standards and guidelines that support an enterprise-wide 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

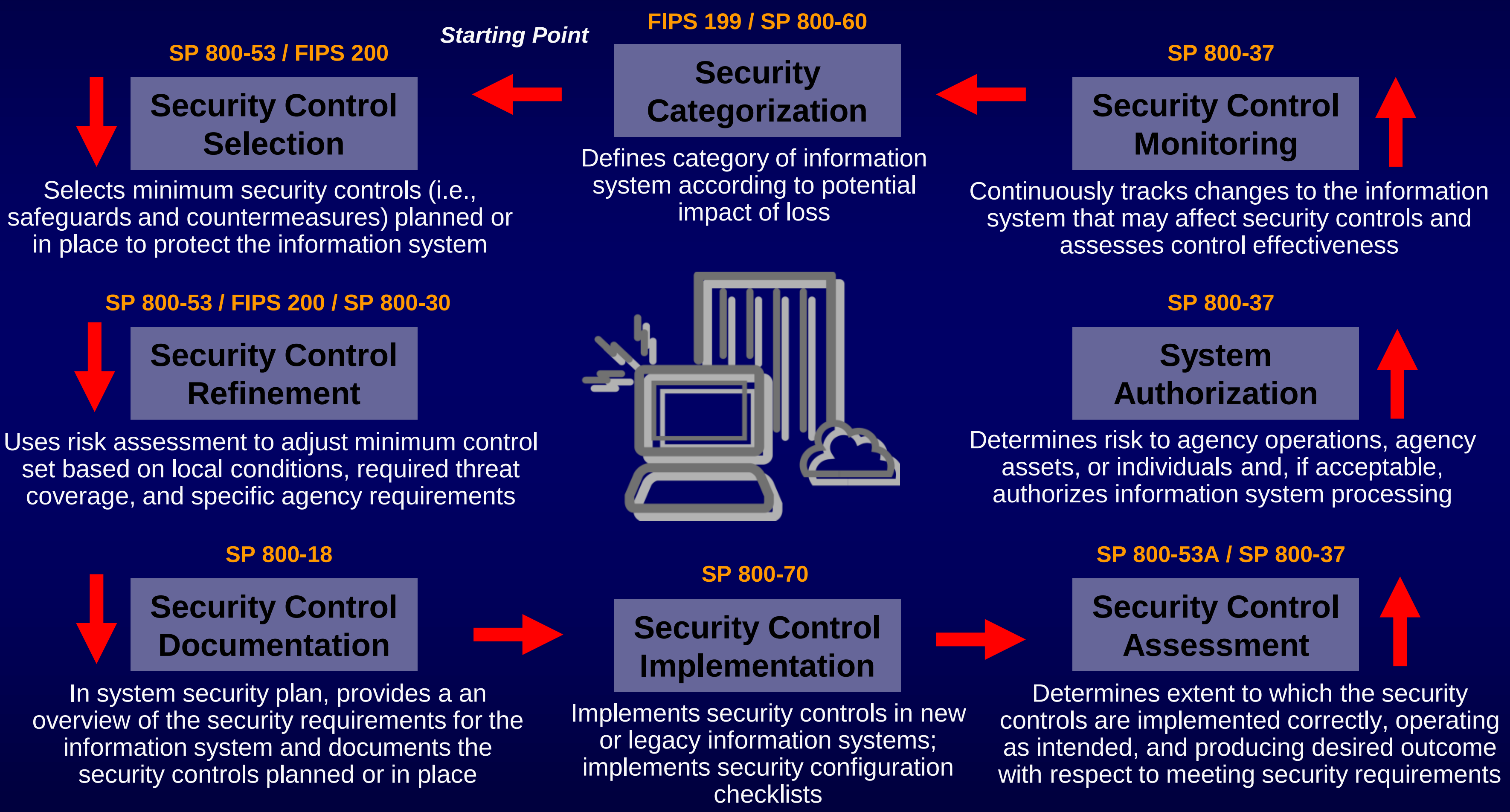
Adversaries attack the weakest link…where is yours?

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk resulting from the operation of an information system:
  - ✓ **Categorize** the information system
  - ✓ **Select** set of minimum (baseline) security controls
  - ✓ **Refine** the security control set based on risk assessment
  - ✓ **Document** security controls in system 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

Managing Enterprise Risk

The Framework



Starting Point

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 / SP 800-30

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

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

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

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

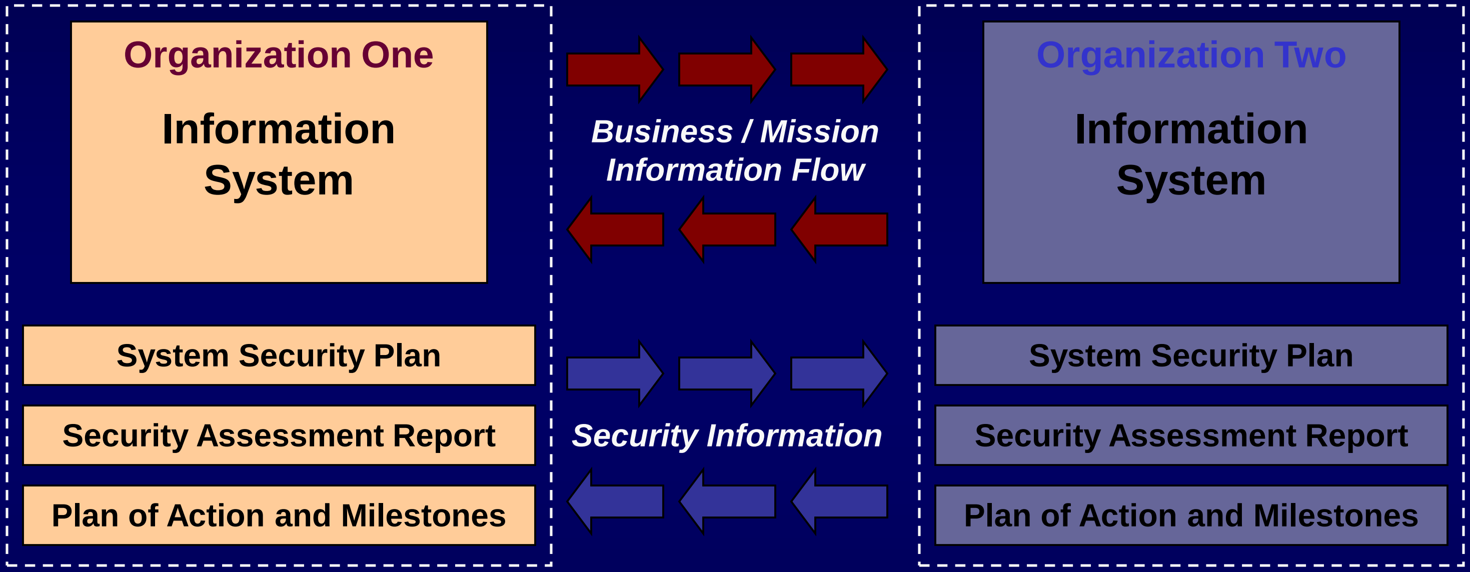
- Don’t be overwhelmed with the enormity or complexity of the information security problem—take one step at a time and build on small successes
- Don’t tolerate indifference to enterprise information security problems

And finally…

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

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.

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

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

Curt Barker
(301) 975-4768
wbarker@nist.gov

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

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

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