Assessment Framework and Methodologies

NIST FISMA Project

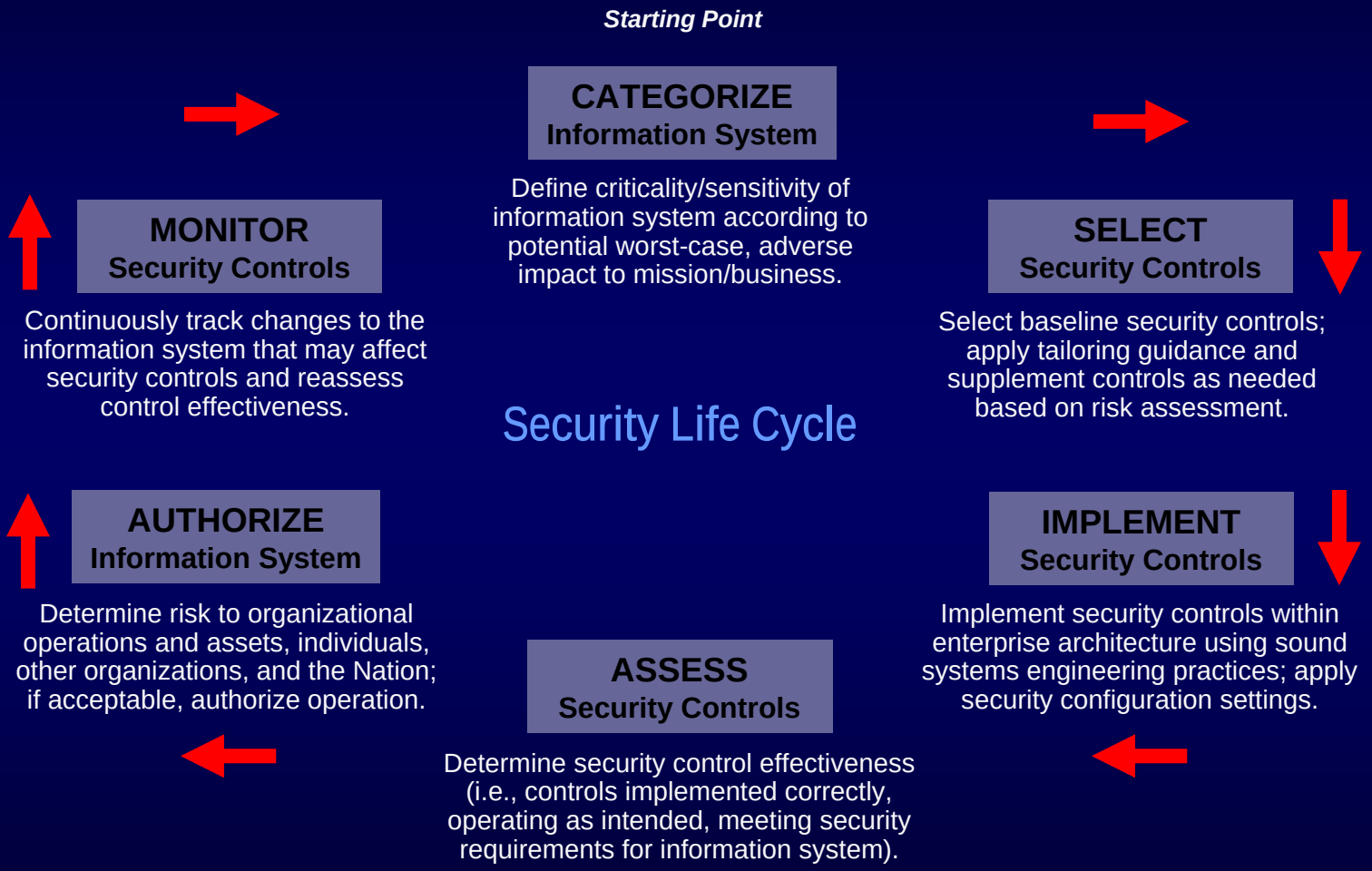
HIPAA Conference

May 18, 2009

Patricia Toth

Computer Security Division
Information Technology Laboratory

Risk Management Framework



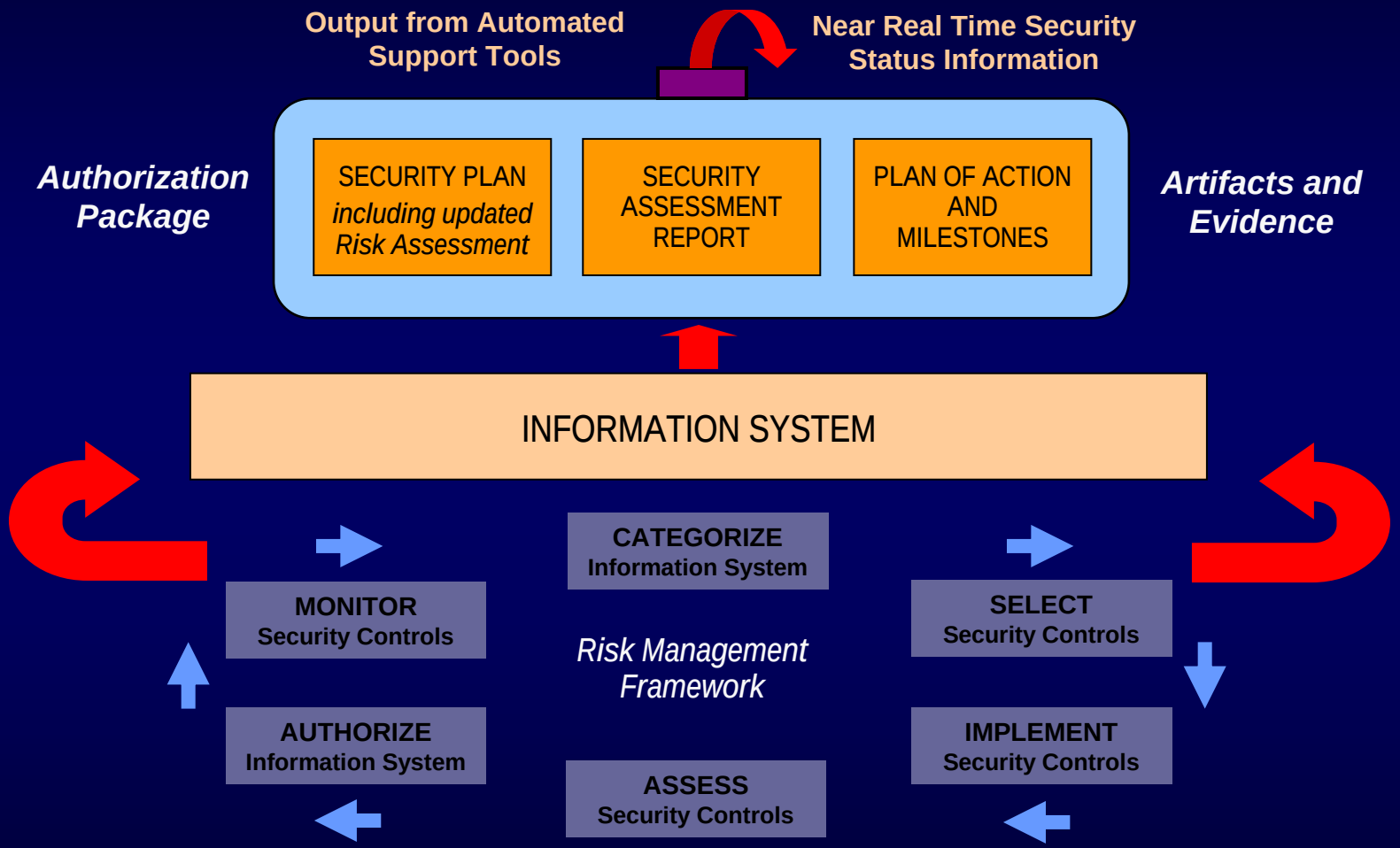
Security Controls

- 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.
- Selecting and Tailoring in terms of the Risk Management Framework.

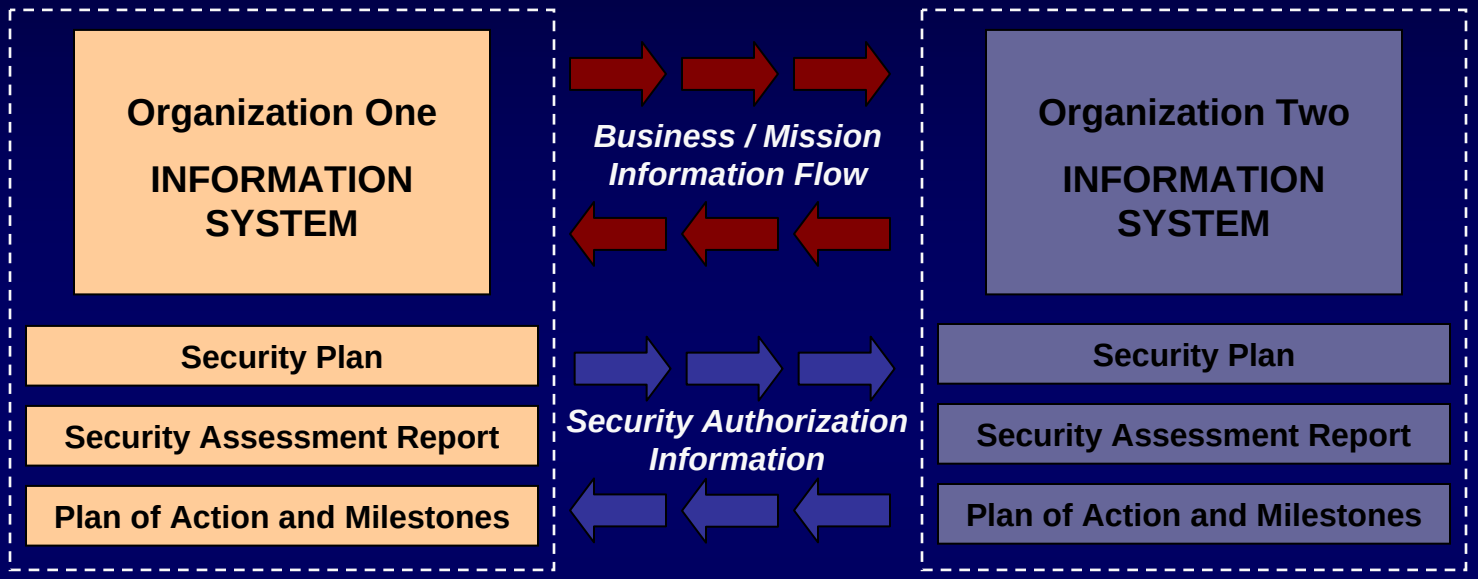
Federal Risk Management Publications

- Security Categorization
  - FIPS 199 (non national security systems)
  - NIST Special Publication 800-60 (non national security systems)
  - CNSS Instruction 1199 (national security systems)
- Security Control Selection
  - FIPS 200 (non national security systems)
  - NIST Special Publication 800-53 (non national security systems)
  - CNSS Instruction 1253 (national security systems)
- Security Control Assessment
  - NIST Special Publication 800-53A (non national security systems)
  - CNSS Instruction 1253A (national security systems)
- Security Authorization
  - NIST Special Publication 800-37 (national security and non national security systems)
- Continuous Monitoring
  - NIST Special Publication 800-53A (non national security systems)
  - CNSS Instruction 1253A (national security systems)
  - NIST Special Publication 800-37 (national security and non national security systems)

Applying the Risk Management Framework to Information Systems



Recognition of Authorization Results



Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

The objective is to achieve transparency of prospective partner's information security authorization processes…establishing trust relationships based on common, shared risk management principles.

FISMA Phase I Publication Status

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) *
- NIST Special Publication 800-39 (Risk Management) **
- 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) *

* Publications currently under revision.
** Publications currently under development.

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.
- A master catalog of security controls for information systems requiring additional threat and risk considerations.

SP 800-53 Fundamentals

- Catalog of security controls
- Security control structure
  - Classes:
    - Management
    - Operational
    - Technical
  - Families (17):
    - Access Control
    - Awareness and Training
    - …….

SP 800-53 Process

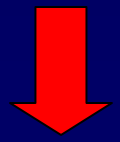
- Categorize information system based on FIPS 199 and SP 800-60:
  - Low Impact;
  - Moderate Impact; or
  - High Impact.
- Selecting initial security control baseline (starting point).
- Tailoring (Scope and Compensate) initial security control baseline.
- Supplement tailored baseline.

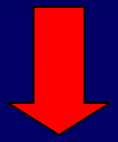
Selecting Minimum Security Controls Sets

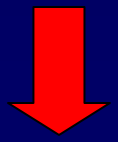
Baselines Provided by Special Publication 800-53

Master Security Control Catalog

Complete Set of Security Controls and Control Enhancements







Minimum Security Controls
Low Impact
Information Systems

Baseline #1

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

Minimum Security Controls
Moderate Impact
Information Systems

Baseline #2

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls, plus additional controls and control ***enhancements***, as needed

Minimum Security Controls
High Impact
Information Systems

Baseline #3

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls, plus additional controls and control ***enhancements***, as needed

Tailoring
(Scoping and Supplementing)

- For each security control baseline (low, moderate, or high) identified in NIST Special Publication 800-53, apply the ***tailoring guidance*** to modify the set of controls to meet the specific operational requirements of the agency.

  Rationale: Application of the tailoring guidance in Special Publication 800-53 can eliminate unnecessary security controls, incorporate compensating controls when needed, and specify agency-specific parameters. Tailoring activities and associated tailoring decisions should be well documented with appropriate justification capable of providing reasoned arguments to auditors.

Scoping Guidance

- Physical Infrastructure-related considerations

  Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system.

- Public access-related considerations

  Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces.

Scoping Guidance II

- Technology-related considerations
  - Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.
  - Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.
  - Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products.

Scoping Guidance II

- Policy/regulatory-related considerations

  Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

Scoping Guidance III

- Scalability-related considerations

  Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected.

- Security objective-related considerations

  Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization before moving to the high water mark; (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.

Compensating Security Controls

- A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system.
- Mission-driven considerations may require alternate solutions (e.g., AC-11 session lock not advisable in certain systems).

Compensating Security Controls

- The organization selects a compensating control from NIST SP 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;
- The organization provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

Supplement

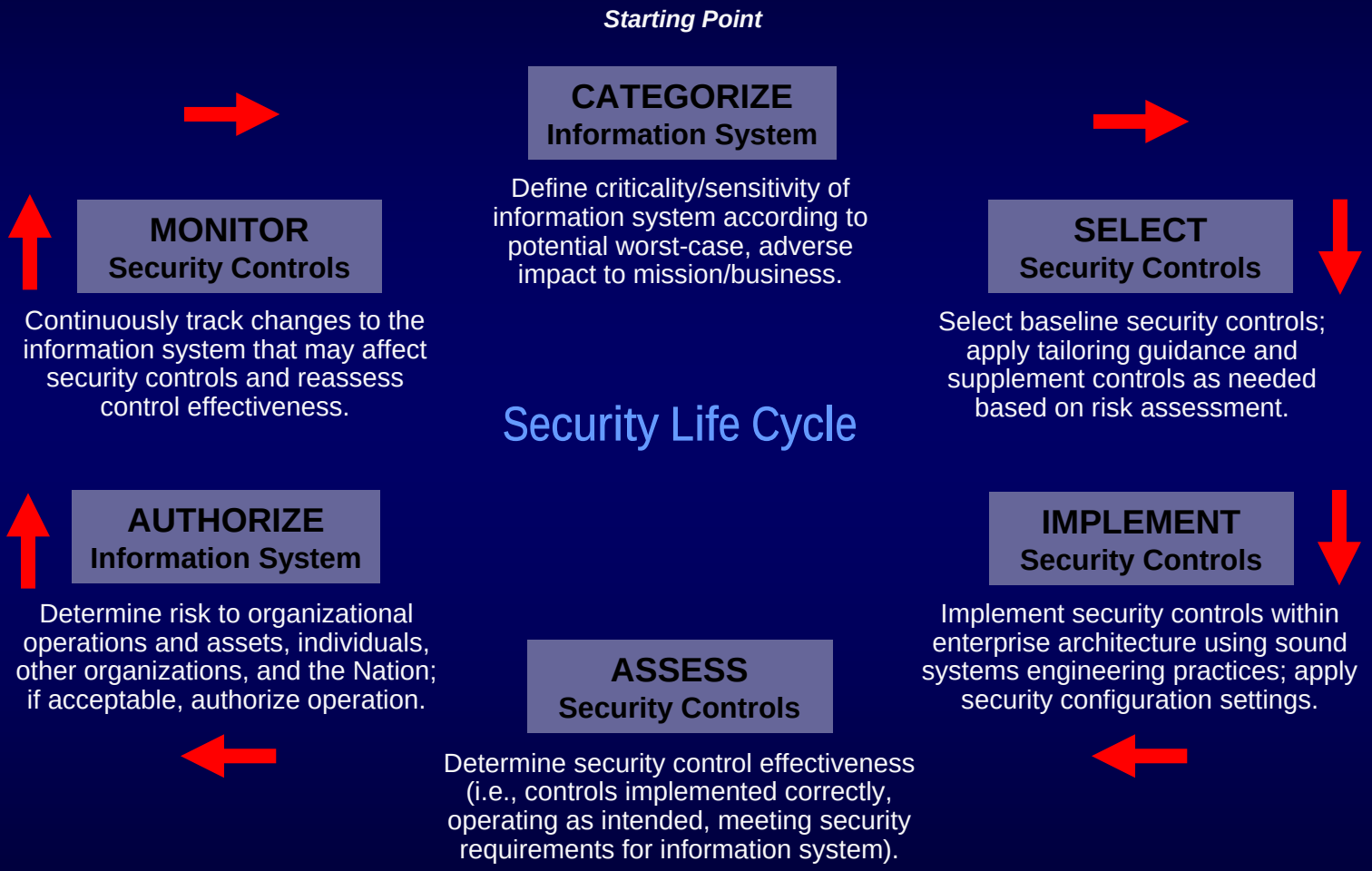
- For each tailored security control baseline, ***supplement*** the security controls with additional controls and/or control enhancements based on the results of an organizational assessment of risk.

Rationale: The tailored baseline represents the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations.

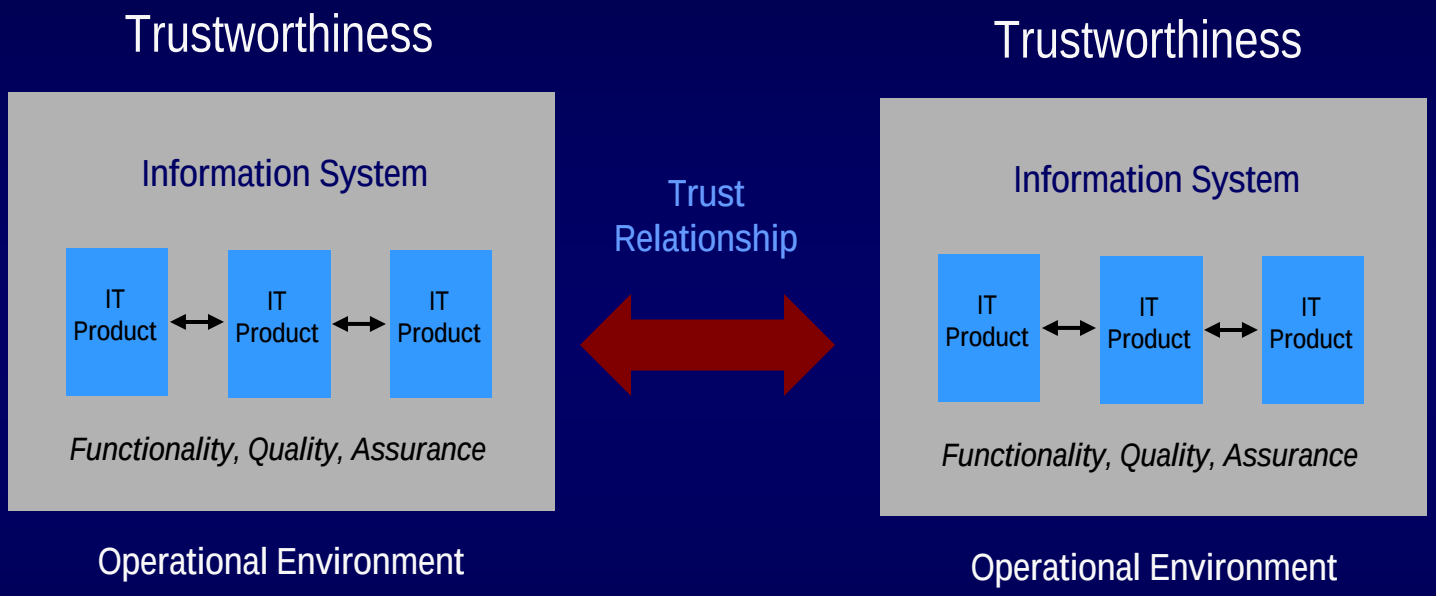
Results In

Set of security controls for the information system that is deemed to provide adequate protection for the particular organization and information system environment.

Risk Management Framework



FISMA Phase II



Producing evidence that supports the grounds for confidence in the design, development, implementation, and operation of information systems.

Training Initiatives

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards, guidelines, programs and services.
- Training initiative includes three components—
  - Frequently Asked Questions
  - Publication Summary Guides (Quickstart Guides)
  - Formal Curriculum and Training Courses

Frequently Asked Questions (FAQs)

- Develop a set of FAQs for each step of the Risk Management Framework
- Categorize and Monitor Steps
  - www.csrc.nist.gov
- Other steps under development

Categorize FAQs

- **General Categorize**
- **Categorization Fundamentals**
- **Organizational Support for the Categorization Process**
- **System-specific Application of the Categorization Process**

General Categorize FAQs

- **What is security categorization and why is it important?**
- Security categorization provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system. The security category is based on the potential impact (worst case) to an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.[1] The information owner/information system owner must identify the types of information associated with the information system and assign a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type.
- The high water mark concept is used to determine the security impact level of the information system for the express purpose of prioritizing information security efforts among information systems and selecting an initial set of security controls from one of the three security control baselines in NIST SP 800-53.[2]
- [1] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 1
- [2] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 17

General Categorize FAQs

- **How is the categorization decision used?**
- Once the overall security impact level of the information system is determined (i.e., after the system is categorized), an initial set of security controls is selected from the corresponding low, moderate, or high baselines in NIST SP 800-53. Organizations have the flexibility to adjust the security control baselines following the scoping guidance, using compensating controls, and specifying organization-defined parameters as defined in NIST SP 800-53. [3] The security category and system security impact level are also used to determine the level of detail to include in security documentation and the level of effort needed to assess the information system.[4]
- [3] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 32
- [4] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008, pp. 9-10

Quick Start Guides

- Each Step of the RMF
  - Categorize and Monitor Steps posted on www.csrc.nist.gov
- Provide a general understanding
- Provided from management, systems and organization perspectives

Quick Start Guides - Categorize

- **Management Perspective**
- **System Perspective**
- **Tips and Techniques for Systems**
- **Organizational Perspective**
- **Tips and Techniques for Organizations**

Training Courses

- RMF Foundation Course
  - 1 day high level overview
  - Pilot course held Dec ’08
- RMF Course
  - 3 day detailed overview
  - Course date TBD
- Wed-based Training

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