FISMA Phase II
Risk Management Training

FISSEA Conference

March 24, 2010

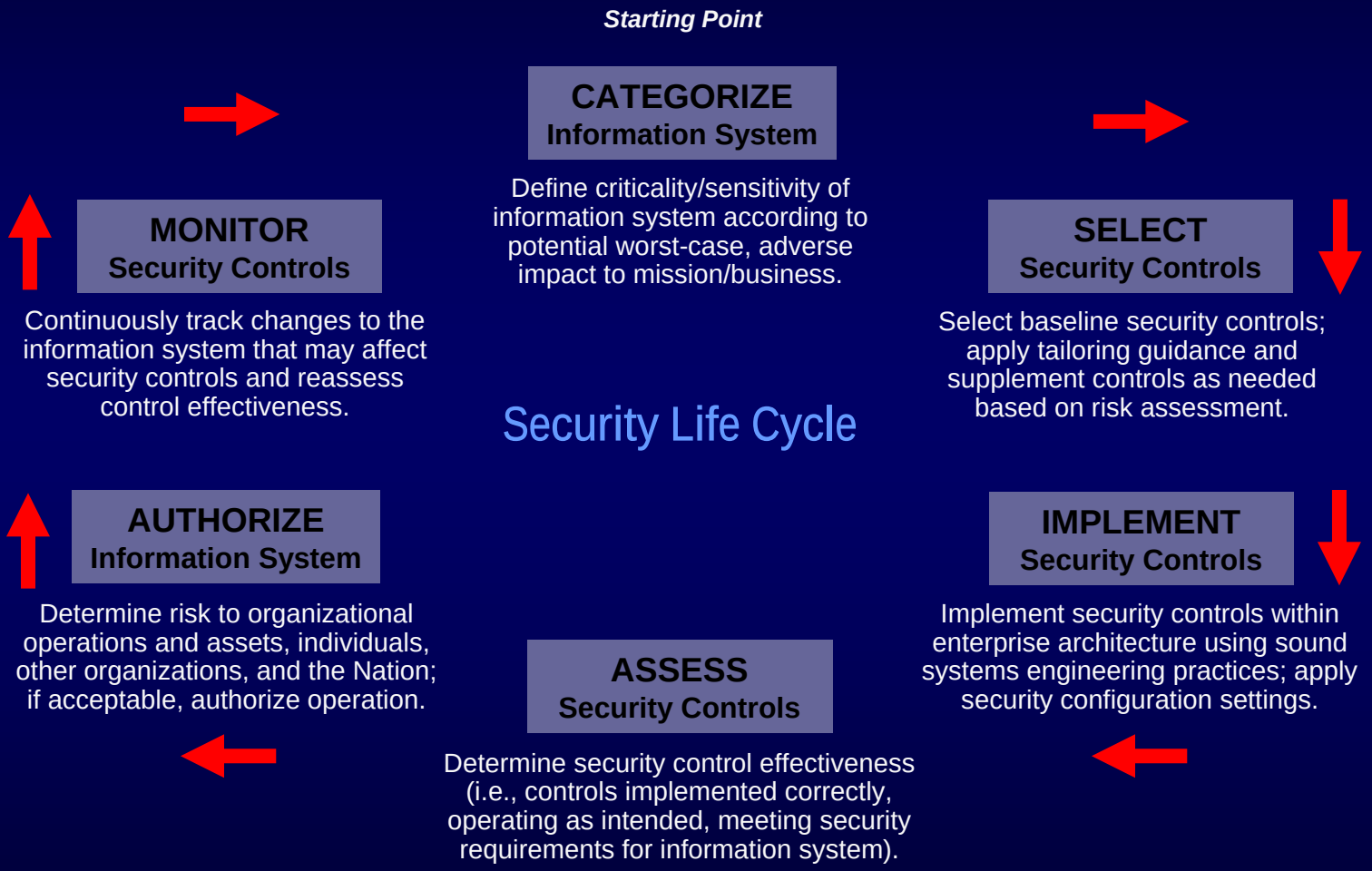
Patricia Toth

Computer Security Division
Information Technology Laboratory

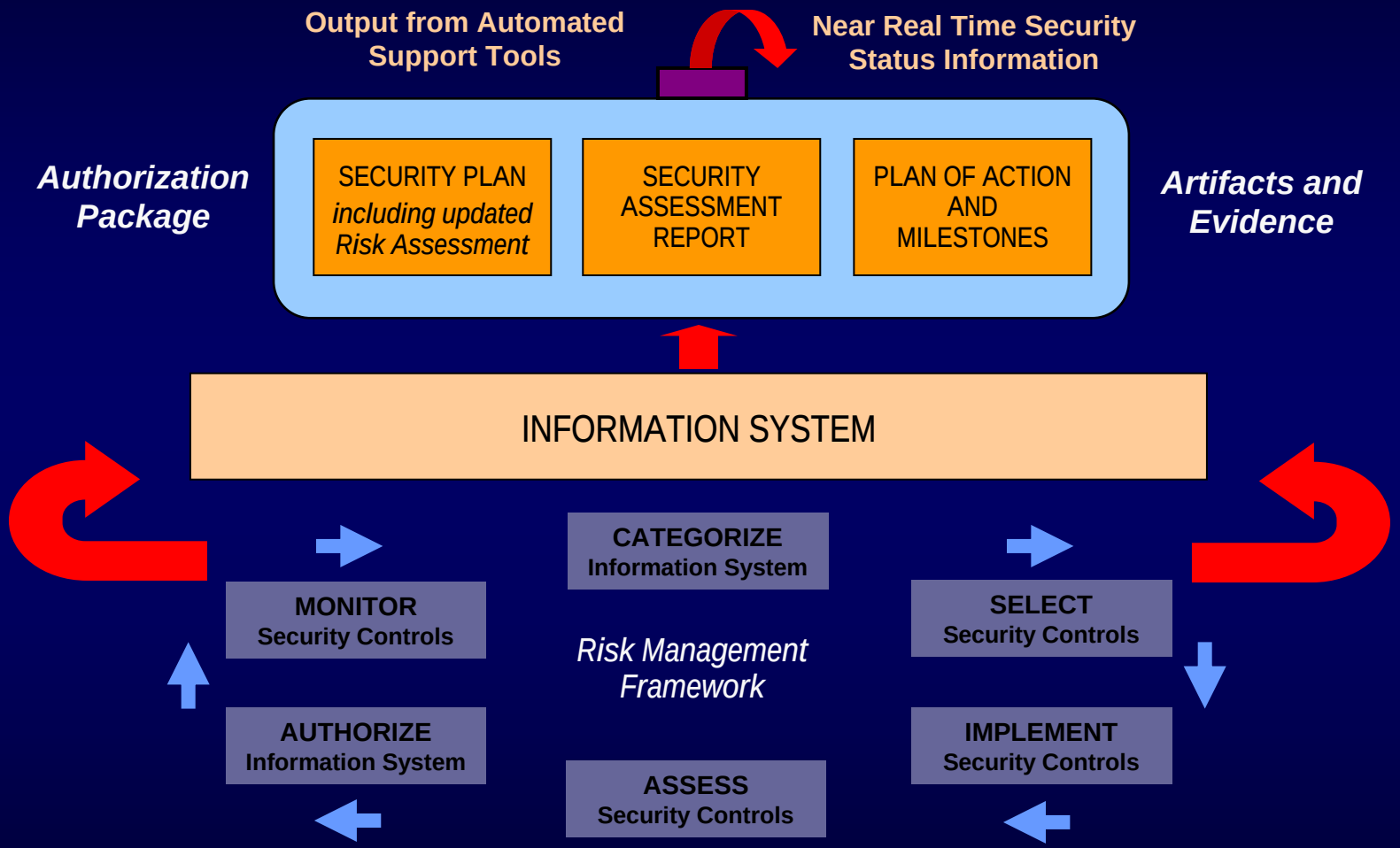
Agenda

- FISMA Phase I
  - *What we have accomplished to date…*
- FISMA Phase II
  - *Where we are headed …*
- Discussion

Risk Management Framework



Applying the Risk Management Framework to Information Systems



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
    - …….

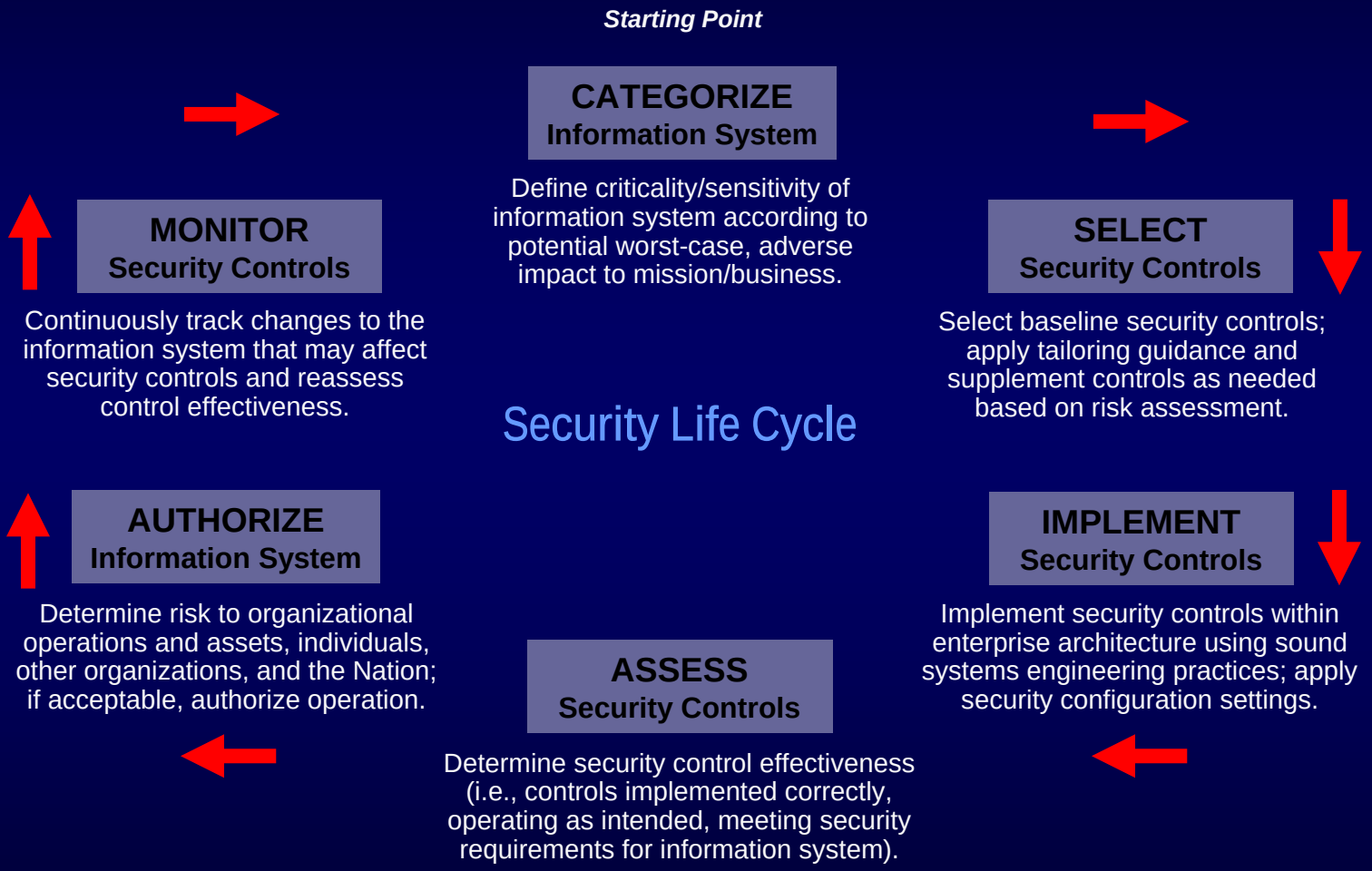
SP 800-53 Process

- 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.

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



Security Control Assessments

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"
  - ✓ Final Publication: July 2008
  - ✓ Assessment Cases: August 2008
  - ✓ NIST Special Publication 800-115, "Technical Guide to Information Security Testing and Assessments"
  - ✓ Final Publication: September 2008

Guidance 800-53A

- Provides common assessment procedures
- Describes repeatable assessment methodology
- Provides guidance for determining if security controls are meeting requirements

Guidance 800-53A cont'd

- Provide guidance for building effective security plans
- Provides guidance for managing assessment results

Organizational Assessment Procedures

- SP 800-53A provides a starting point for developing specific procedures
- Maximize flexibility, promote consistent, comparable and repeatable assessments
- Supplemented, as needed

Benefits of RMF Assessment Methodology

- Minimizes risks
- Addresses resource constraints
- Provides re-usability of pre-established resources
- Decreases time
- Produces documentation for security assessment reports
- Reduces overall costs

Guidance SP 800-115

- A guide to basic technical aspects of conducting information security assessments
- Presents technical testing and examination techniques

Guidance SP 800-115 cont'd

Recommends assessment activities:

- Prepare for assessment
- Develop assessment procedures
- Develop security assessment plan
- Carry out assessment
- Document the assessment

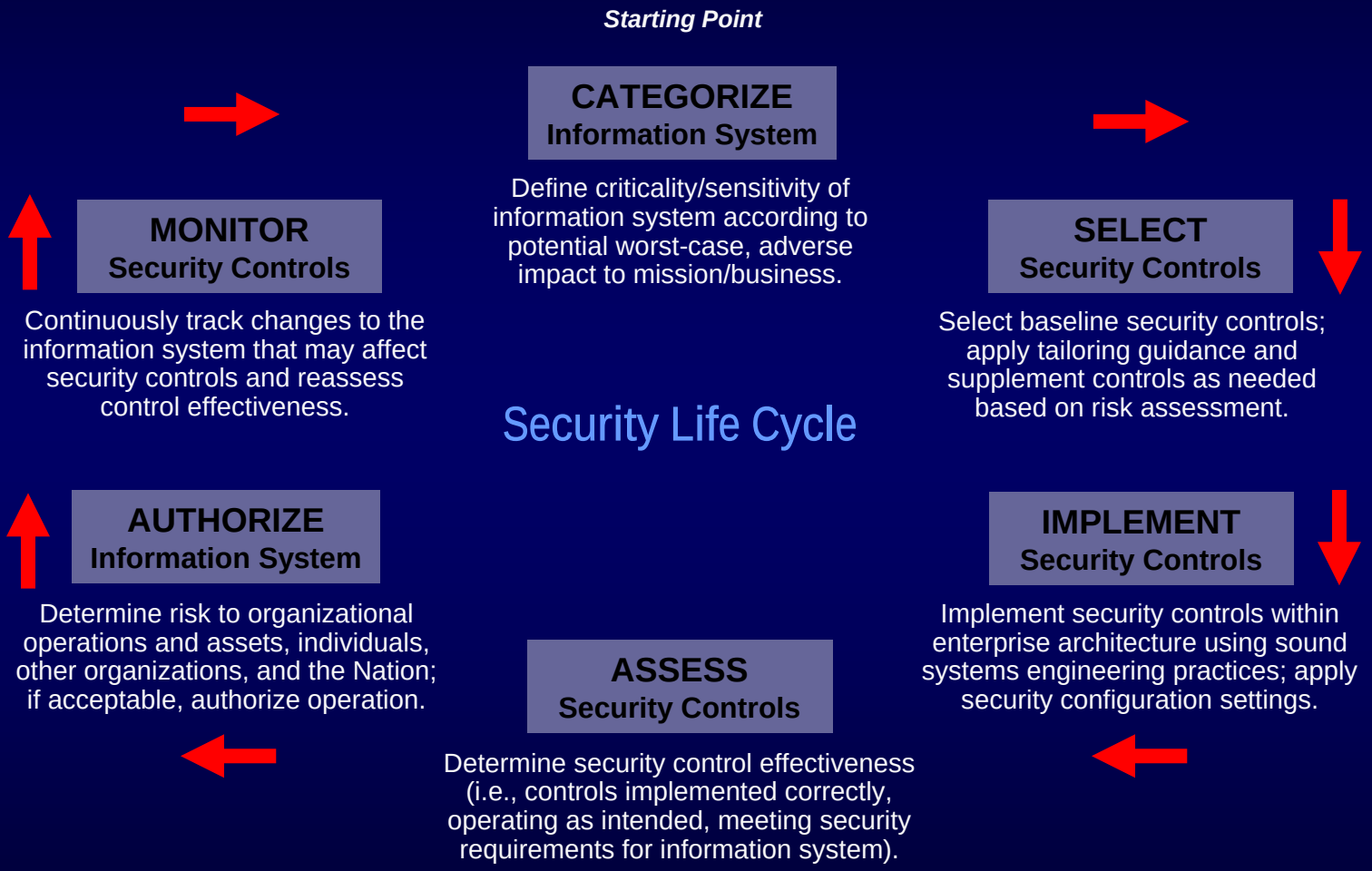
Assessment Methods

- Review
- Examine
- Test

Documentation

- Security Assessment Reports
  - Level of detail
  - Consistent with policy, guidance and requirements
  - Type of assessment conducted
  - Findings influence system security plan, POAM and steps required to correct

Risk Management Framework



Goals of Continuous Monitoring

- Determine if controls are effective over time
- Provide near real-time security status
- Enable officials to make risk-based decisions

Guidance SP 800-37

- Develop strategy
- Document changes
- Perform impact analysis
- Conduct on-going assessments and remediation actions
- Document updates and status reporting
- Active involvement by authorizing officials

Implementing a Continuous Monitoring Program

- Security Impact Analysis
  - Analyze changes
  - Determine impact to controls in place
  - Determine if new vulnerabilities exist
  - Initiate corrective actions
  - Revise system security plan, security assessment report and POAM

Implementing a Continuous Monitoring Program

- Ongoing Security Control Assessments
  - Assess all controls during initial authorization
  - Assess a subset annually
  - Periodically assess a subset of controls
    - Subset and frequency determined by system owner

Implementing a Continuous Monitoring Program

- Ongoing Remediation Actions
  - Review security assessment report to initiate remediation actions of outstanding POAM items
  - Re-assess controls

Implementing a Continuous Monitoring Program

- Critical Document Updates
  - Security Plans
  - Security Assessment Report
  - POAMs

Implementing a Continuous Monitoring Program

- Security Status Reporting
  - Provide status
  - Describe continuous monitoring activities
  - Address vulnerabilities
  - Summarize key changes to Security Plans, Security Assessment reports and POAMs

Implementing a Continuous Monitoring Program

- On-going Risk Determination and Acceptance
  - Authorizing Official
    - Reviews reported security status periodically
    - Determines whether risk is acceptable

Implementing a Continuous Monitoring Program

- System Removal and Decommissioning
  - Ensure implementation of all controls related to decommissioning
  - Update tracking and management systems
  - Reflect new status in security status report
  - Notify users and application owners
  - Assess any security control inheritance relationships

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

Organizational Credentialing Initiatives

- Draft NISTIR 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems* (September 2007).
- Draft Criteria for Product & Service Supplier Claims Statement

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
  - Select – May 2010
  - Assess – July 2010

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
- Select – May 2010

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 courses held Dec ’08, Nov ’09
  - Presented at various Conferences
  - DOE Cyber Security May 2010
- RMF Course
  - 3 day detailed overview course
  - Course date TBD
- Wed-based Training – April ‘10

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