

NIST Special Publication 800-53

Recommended Security Controls for Federal Information Systems

A Status Report

Ron Ross

*Computer Security Division
Information Technology Laboratory*

A Brief Review

Question

How does security control selection fit into an agency's information security program?

A Brief Review

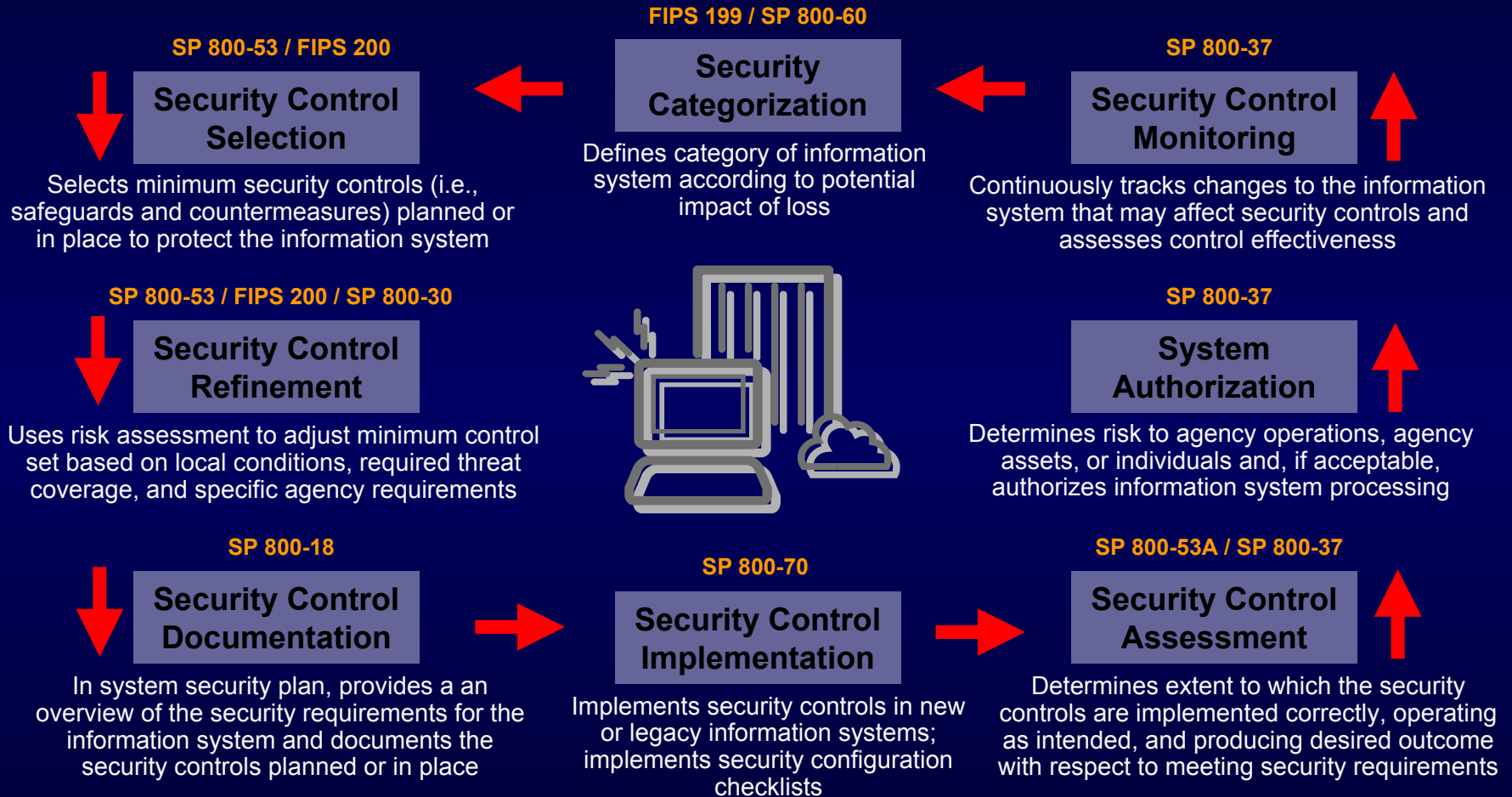
Answer

Security control selection is an important activity that supports a risk management process and is an integral part of an agency's overall information security program

Managing Agency Risk

- Key activities in managing **agency-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

Risk Management Framework



Strategy for Revising Special Publication 800-53

Key Development Concepts

- There will be a clear and distinct separation of security control developer/implementer requirements and security control assessor requirements
- There will be three security control types defined within the master catalog of controls including:
 - Documentation-based controls
 - Activity-based controls
 - Mechanism-based controls

Key Development Concepts

- Security controls will be defined at the token requirement level, (i.e., a single requirement per control)
- Enhanced and strong versions of security controls will be developed on an as needed basis
- There will be one group of assessment methods and associated assessment procedures for each security control in the master catalog of controls

Revised Document Structure

- Introduction
 - *The context for the importance of security controls—relating to key legislative and policy drivers*
- The Fundamentals
 - *The structure and types of security controls, organization of the master control catalog, methods to instantiate control variables*
- The Process
 - *The process of selecting a baseline set of security controls using FIPS Publication 199 and its relationship to the organization's risk management process*
- Appendices
 - *Low, moderate, and high security control baselines, master control catalog, other supporting information*

New Security Control Structure

- Simplified structure consisting of:
 - Token-level security control statement
 - Supplemental guidance

- Example:

FAMILY: CONTINGENCY PLANNING AND OPERATIONS (CP)

Contingency Planning

CP-1 CONTINGENCY PLAN DEVELOPMENT

CP-1.b Basic Control: The organization develops a contingency plan for the information system consistent with the intent of NIST Special Publication 800-34, addressing as a minimum, identification and notification of key personnel, plan activation, system recovery, and system reconstitution.

Supplemental Guidance: The level of detail provided in the contingency plan should be commensurate with the security category of the information system in accordance with FIPS Publication 199.

Development Phases

- Develop basic security controls for master catalog
- Develop build criteria for enhanced and strong security controls
- Develop enhanced and strong security controls (where needed) for the master catalog
- Establish baselines (minimum security controls) for low, moderate, and high impact systems

Projected Publication Schedule

- Special Publication 800-53
Second Public Draft, August 2004
- Special Publication 800-53
Third Public Draft, January 2005
- Special Publication 800-53
Final Publication, March 2005

Note: Special Publication 800-53 will transition into FIPS 200 not later than December 2005. Several publication options under consideration.

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 (Assessment Methods/Procedures)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)
- FIPS Publication 200 (Minimum Security Controls)

Publication Completed 

Publication in Development 

Contact Information

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

Project Manager

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

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

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

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

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

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

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

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