NIST Risk Management Framework

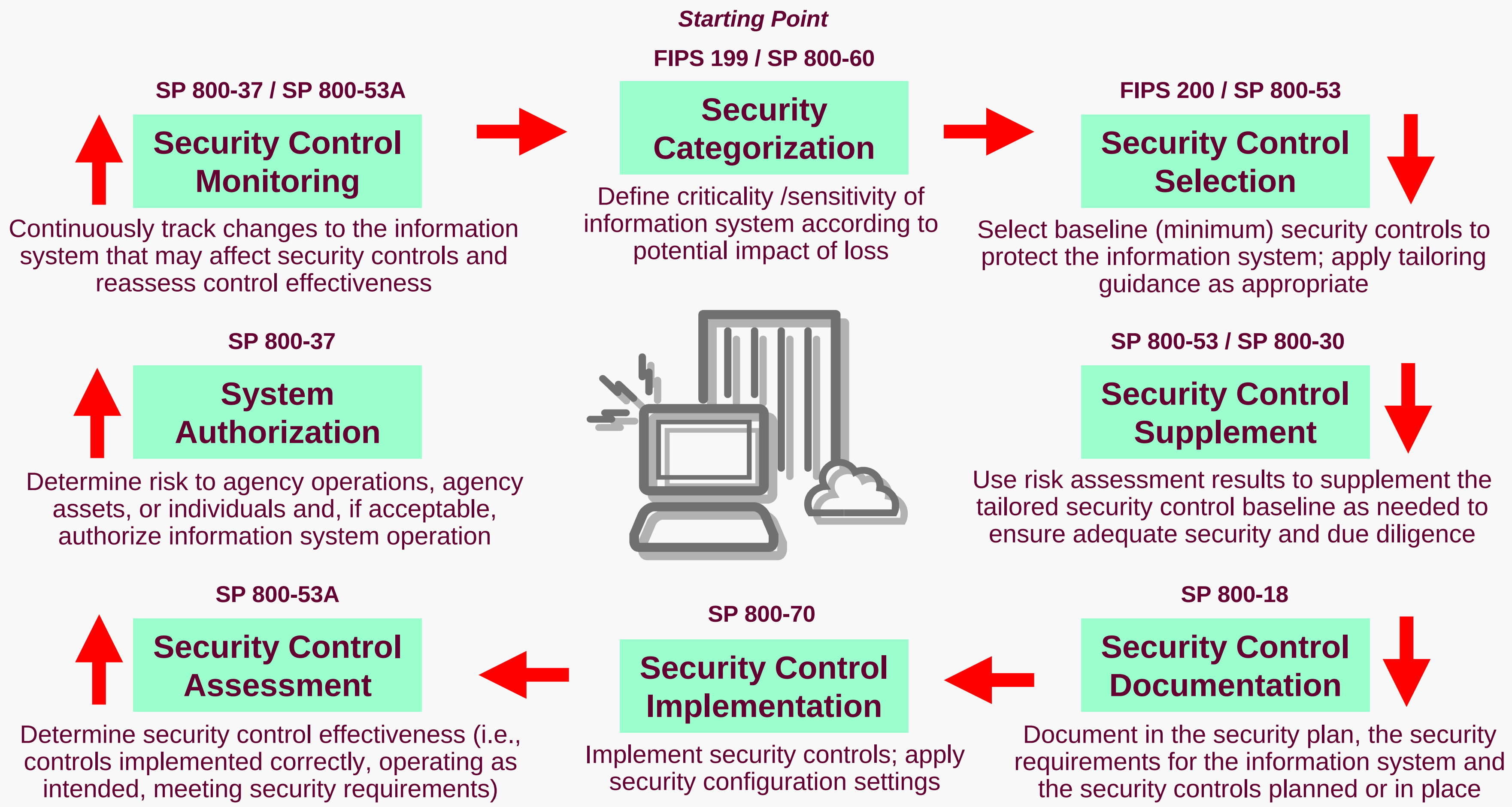
Computer Security Division
Information Technology Laboratory

National Institute of Standards and Technology

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk to the enterprise and to other organizations resulting from the operation of an information system:
  - ✓ Categorize the information system (criticality/sensitivity)
  - ✓ Select and tailor baseline (minimum) security controls
  - ✓ Supplement the security controls based on risk assessment
  - ✓ Document security controls in system security plan
  - ✓ Implement the security controls in the information system
  - ✓ Assess the security controls for effectiveness
  - ✓ Authorize information system operation based on mission risk
  - ✓ Monitor security controls on a continuous basis

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

Security Categorization

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-53 / SP 800-30

Security Control Supplement

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Security Control Documentation

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Security Control Implementation

Implement security controls; apply security configuration settings

SP 800-53A

Security Control Assessment

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

System Authorization

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

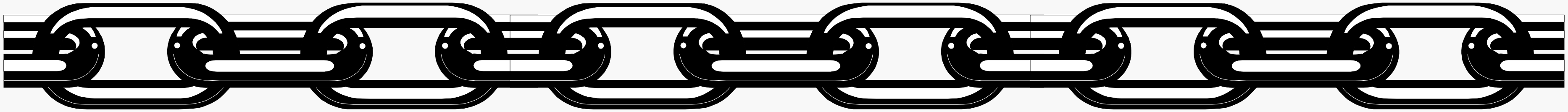
SP 800-37 / SP 800-53A

Security Control Monitoring

Continuously track changes to the information system that may affect security controls and reassess control effectiveness

National Institute of Standards and Technology

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
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation

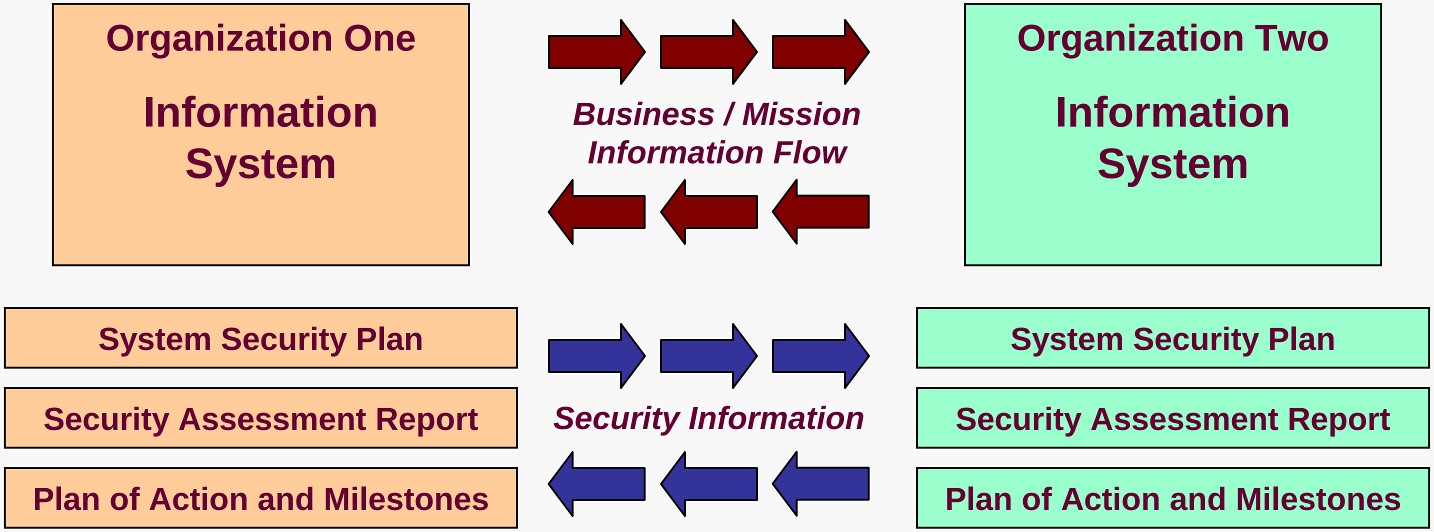
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms
  (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices
  (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

National Institute of Standards and Technology

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 and trust.

National Institute of Standards and Technology

Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (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)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation…

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

Matt Scholl
(301) 975-2941
matthew.scholl@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