


Chapter 15: Security Controls and Plans

FISMA and NIST

- **FISMA** – Federal Information Security Management Act
 - Law enacted by Congress - part of the E-Gov Act of 2002
 - Applies to federal organizations and their contractors
 - Requires implementation of “information security protections commensurate with the risk and magnitude of the harm”
- **NIST** – National Institute of Standards and Technology
 - FISMA requires NIST to develop standards and guidelines to help federal organizations improve the security of federal information and information systems (and implement FISMA)
- NIST publications – <http://csrc.nist.gov/publications>

Directives and NIST

- **OMB** – Office of Management and Budget
 - Directives in the form of Memos and Circulars (usually)
 - May mandate NIST guidance for use by federal organizations
 - **EOs and PDs** – Executive Orders and Presidential Directives
 - Directives from the Executive Office of the President
 - May direct NIST to provide guidance or develop a standard
 - **HSPD** – Homeland Security Presidential Directive
 - An Executive Order focused on ensuring homeland security with implementation usually managed by DHS
 - Example: HSPD-12 which calls
- Hacked in 2015. So much for mandating NIST guidance
- 

Joint Task Force Transformation Initiative

- A Broad-Based Partnership —
 - National Institute of Standards and Technology
 - Department of Defense
 - Intelligence Community
 - Office of the Director of National Intelligence
 - 16 U.S. Intelligence Agencies
- Committee on National Security Systems

Standards/Guidelines for FISMA & RM

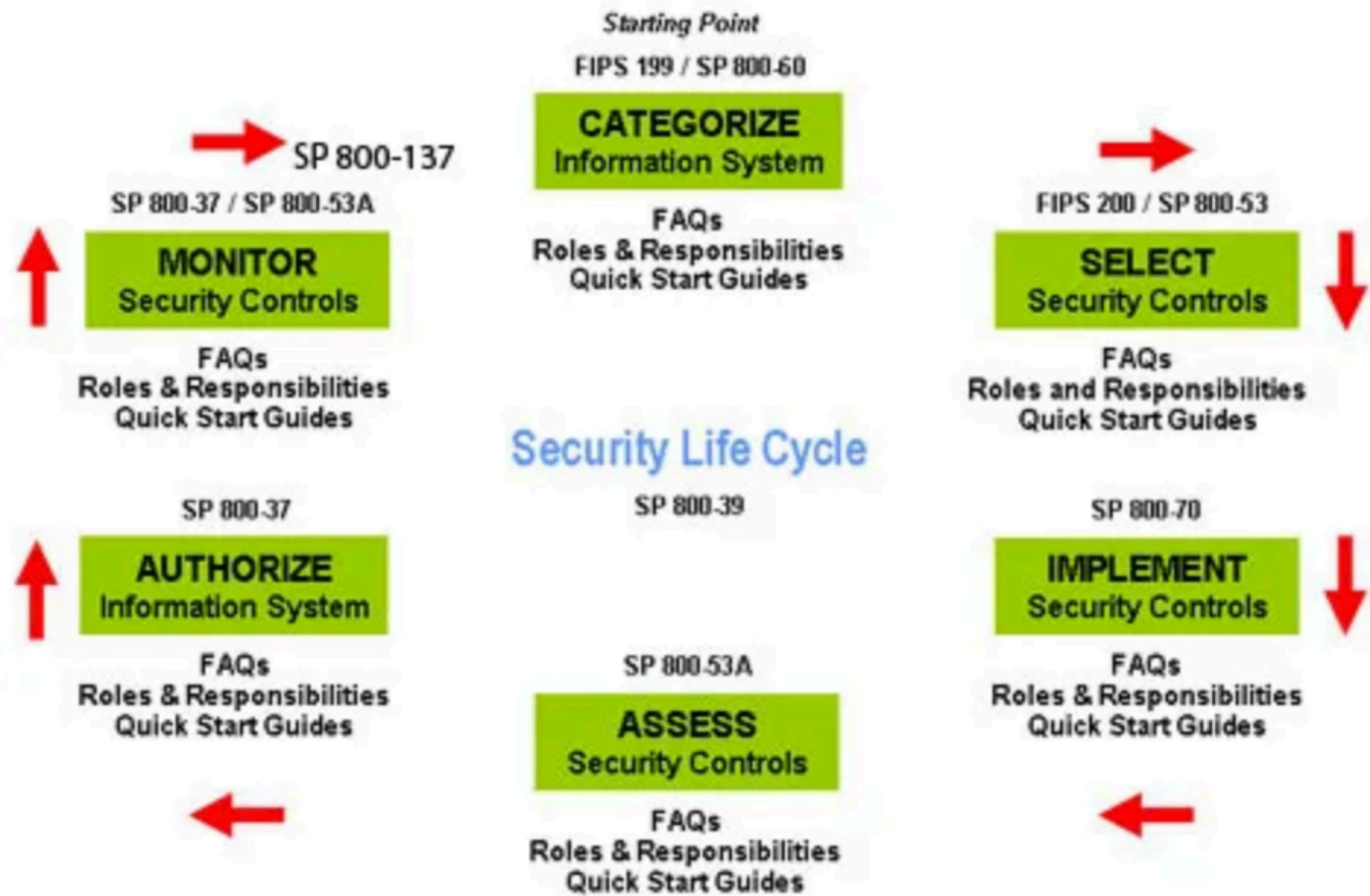
- FIPS - Federal Information Processing Standards
 - FIPS 199 – Standards for Security Categorization
 - FIPS 200 – Minimum Security Requirements
- SPs – Special Publications
 - SP 800-18 – Guide for System Security Plan development
 - SP 800-30 – Guide for Conducting Risk Assessments
 - SP 800-34 – Guide for Contingency Plan development
 - SP 800-37 – Guide for Applying the Risk Management Framework
 - SP 800-39 – Managing Information Security Risk
 - SP 800-53/53A – Security controls catalog/assessment procedures
 - SP 800-60 – Mapping Information Types to Security Categories
 - SP 800-128 – Security-focused Configuration Management
 - SP 800-137 – Information Security Continuous Monitoring
 - Many others for operational and technical implementations

NIST SP 800-37

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- A holistic risk management process
 - Integrates the RMF into the SDLC
 - Provides processes (tasks) for each of the six steps in the Risk Management Framework at the system level

RMF Cycle to Standard



Step 1: Categorize

FIPS 199: Standards for Security Categorization of Federal Information and Information Systems

- Supports Step 1 (Categorize) of the RMF
- In the context of [security objectives](#) from FISMA
 - [Confidentiality](#) – unauthorized disclosure
 - [Integrity](#) – unauthorized modification/destruction
 - [Availability](#) – disruption of access to/use of information
- Defines three impact levels:
 - [Low](#) – loss would have a **limited** adverse impact
 - [Moderate](#) – loss would have a **serious** adverse impact
 - [High](#) – loss would have a **catastrophic** adverse impact

NIST Special Publication 800-60:

Guide for Mapping Types of Information and Information Systems to Security Categories

- Supports Step 1 (Categorize) of the RMF
 - Volume 1 provides guidance
 - Volume 2 provides a catalog of information types and provisional categorizations (impact levels)
 - Low
 - Moderate
 - High
- The standard for impact levels is FIPS 199

NIST Special Publication 800-18:

Guide for Developing Security Plans for Federal Information Systems

Part 4 of
AeroTech Drone
Project

- Guidance for developing **System Security Plan** (SSP)
 - Structure and content
 - Template
- Supports all RMF steps, but begins during Step 1
- Used to record information about the system
 - System boundary/diagram
 - Roles and responsibilities
 - Security control implementation details

Step 2: Select

Part 3 of
AeroTech Drone
Project

FIPS 200: Minimum Security Requirements for Federal Information and Information Systems

- Defines 17 security-related areas (families) that:
 - Represent a broad-based, balanced security program
 - Include management, operational, and technical types of controls (all are needed for defense in depth)
- Specifies implementation of minimum baseline of security controls, as defined in NIST SP 800-53
- Specifies that the baselines are to be appropriately tailored

NIST Special Publication 800-53

Security and Privacy Controls for Federal Information Systems and Organizations

- A [catalog](#) of security controls
 - Supports Step 2 (Select) of the RMF
 - Defines three security baselines (L, M, H)

Security Controls

- The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
- 800-53 defines three types of controls:
 - Common controls
 - System specific controls
 - Hybrid controls

Control Families

ID	FAMILY	ID	FAMILY
<u>AC</u>	Access Control	<u>PE</u>	Physical and Environmental Protection
<u>AT</u>	Awareness and Training	<u>PL</u>	Planning
<u>AU</u>	Audit and Accountability	<u>PM</u>	Program Management
<u>CA</u>	Assessment, Authorization, and Monitoring	<u>PS</u>	Personnel Security
<u>CM</u>	Configuration Management	<u>PT</u>	PII Processing and Transparency
<u>CP</u>	Contingency Planning	<u>RA</u>	Risk Assessment
<u>IA</u>	Identification and Authentication	<u>SA</u>	System and Services Acquisition
<u>IR</u>	Incident Response	<u>SC</u>	System and Communications Protection
<u>MA</u>	Maintenance	<u>SI</u>	System and Information Integrity
<u>MP</u>	Media Protection	<u>SR</u>	Supply Chain Risk Management

SP 800-53 Baselines

- Baselines are defined in Appendix D, Table D-2
- Baselines are determined by:
 - Information and system categorization (L, M, H)
 - Organizational risk assessment and risk tolerance
 - System level risk assessment
- Baselines are a starting point and should be tailored to fit the mission and system environment
 - Parameters
 - Scoping/Compensating
 - Supplementing

Security Controls

- **Compensating Control** - The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

Compensating Controls

- Where a sufficient level of trust cannot be established in the external services and/or providers, organizations can: (i) **mitigate** the risk by employing **compensating controls**; (ii) **accept** the risk within the level of organizational risk tolerance; (iii) **transfer** risk by obtaining insurance to cover potential losses; or (iv) **avoid** risk by choosing not to obtain the services from certain providers (resulting in performance of missions/business operations with reduced levels of functionality or possibly no functionality at all).
- For example, in the case of cloud-based information systems and/or services, organizations might require as a compensating control, that all information stored in the cloud be encrypted for added security of the information.

View the Baselines

Why are Some Controls NOT in Baselines?

- 800-53 provides a comprehensive set of security controls, BUT every system does not need to implement every control (risk management)
- Controls and enhancements not selected in a baseline are available as [compensating](#) or [supplemental](#) controls to strengthen the level of protection IAW:
 - Assessment of risk for the system and environment of operation; and
 - Organizational risk tolerance
 - Overlay requirements for specific communities

How Do I Implement The Controls?

Control Correlation Identifier (CCI)

- The Control Correlation Identifier (CCI) provides a standard identifier and description for each of the **singular, actionable, measurable** statements that comprise an IA control or IA best practice.
- CCI bridges the gap between high-level policy expressions and low-level technical implementations.

CCI Review

Security Control Traceability Matrix (SCTM)

Part 3 of
AeroTech Drone
Project

- Helps identify gaps in security controls
- Tracks security control implementation over time
- Ensures compliance with regulations
- Provides a comprehensive view of a system's security posture

SCTM Review

Step 3: Implementing

SP 800-37R1

- Follow Step 3 tasks in SP 800-37R1
 - Many publications are available to provide implementation guidance on a wide range of controls and control types (csrc.nist.gov)
 - Many automated tools are available to implement specific controls
 - Plan for control implementation during the development phase of the SDLC – **BAKE IT IN**

Security Technical Implementation Guides (STIGs)

- Contains all requirements that have been flagged as applicable for the product which have been selected on a baseline.
- Automates the application of many controls for covered products

STIG Demo