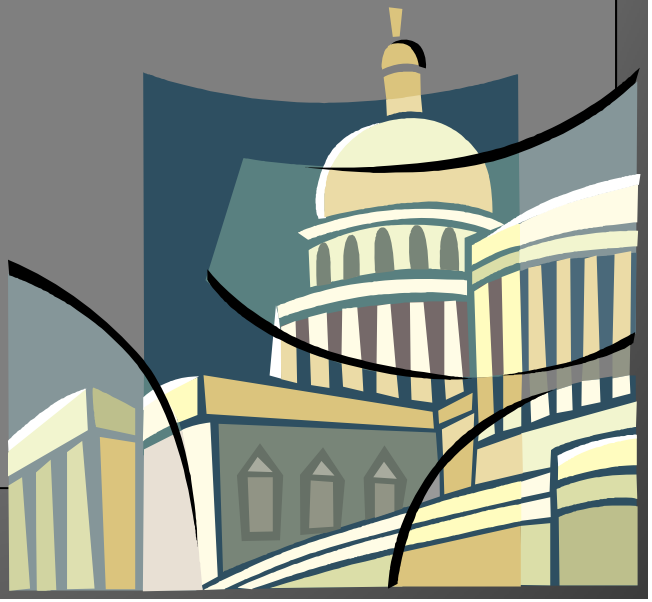
NIST 800-37 Rev 1: What's the same, what's changed?

5/24 ASQ/SSQ/IEEE CS Meeting

Legislation

- Federal Information Security Management Act of 2002
  - "…develop, document, and implement an agency-wide information security program…"
  - Designates NIST as Executive Agent for developing information security guidance for federal agencies
- OMB Circular A-130
  - Plan for security
  - Assign security responsibility
  - Authorize system processing
  - Adhere to NIST guidance



Changes

- C&A => A&A (as part of RMF)
- Harmonization of CNSS, DoD, IC, and civilian processes
- System Risk => Organizational Risk
- MA, GSS => Domain, Dynamic and External Subsystems
- Application => Information System
- Resiliency
- Paperwork Exercise?
- Continuous Monitoring???

Definitions of Applicable Terms

Definitions of Applicable Terms

- Certification = (Security Control) Assessment

~~Certification is a comprehensive assessment~~ Testing and/or evaluation of the management, operational, and technical security controls in an information system~~, made in support of security accreditation,~~ to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- Accreditation = Authorization

~~Accreditation is~~ the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, *other organizations, and the Nation* based on the implementation of an agreed-upon set of security controls.

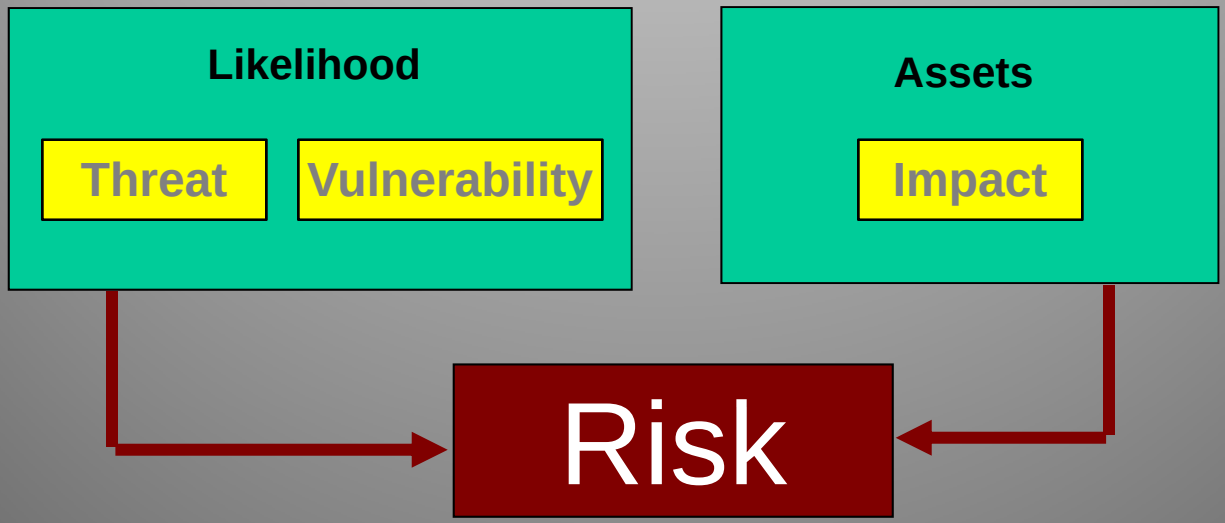
Definitions of Applicable Terms

- Asset: People, information, business resource, process, product, IT infrastructure, reputation, etc.
- Threat: Potential natural or man-made event having an undesirable impact on the business mission
- Safeguard: Control or countermeasure employed to reduce a risk
- Vulnerability: Absence or weakness of a safeguard

Definitions of Applicable Terms

- Authorization Boundary:
  - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
  - For additional definitions of terms see NIST IR 7298

Definitions of Applicable Terms



Security Goals

Security Goals

- **Confidentiality** - A requirement that private or confidential information not be disclosed to unauthorized individuals.
- **Integrity** - A requirement that information and programs are changed only in a specified and authorized manner.
- **Availability** - A requirement intended to assure that systems work promptly and service is not denied to authorized users

FIPS 199 - Potential Impact

The *potential impact* is [**LOW/MODERATE/HIGH**] if—

- The loss of confidentiality, integrity, or availability could be expected to have a [**limited/serious/severe or catastrophic**] adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A [**limited/serious/severe or catastrophic**] adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a [**degradation/ significant degradation/ severe degradation**] in mission capability to an extent and duration that the organization [**is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced/ is able to perform its primary functions, but the effectiveness of the functions is significantly reduced/ is not able to perform one or more of its primary functions**]; (ii) result in [**minor/significant/major**] damage to organizational assets; (iii) result in [**minor/significant/major**] financial loss; or (iv) result in [**minor harm to individuals/significant harm to individuals that does not involve loss of life /or serious life threatening injuries/severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries**].

Security Category

SC information type =

{(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

High Water Mark

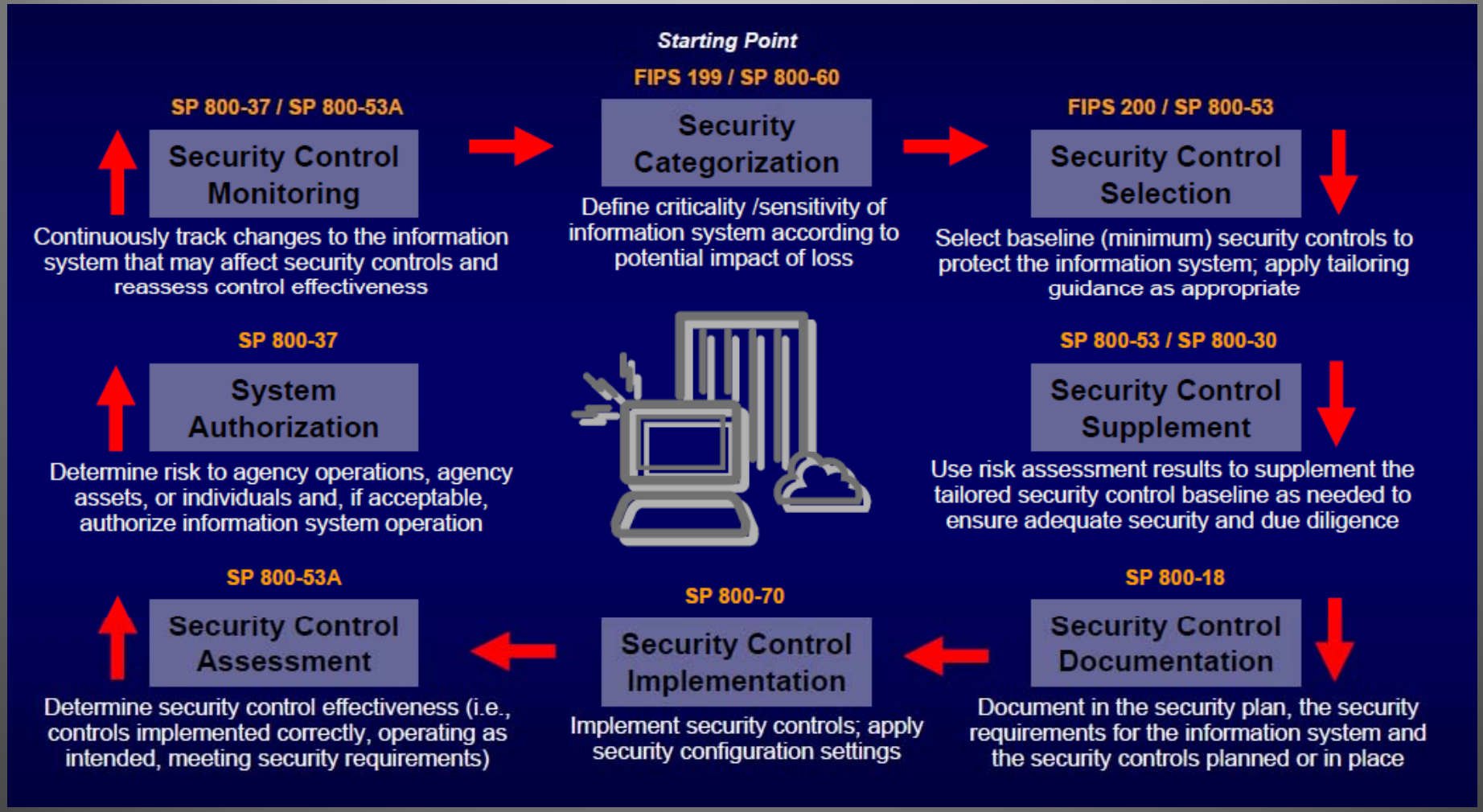
SC information system =

{(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

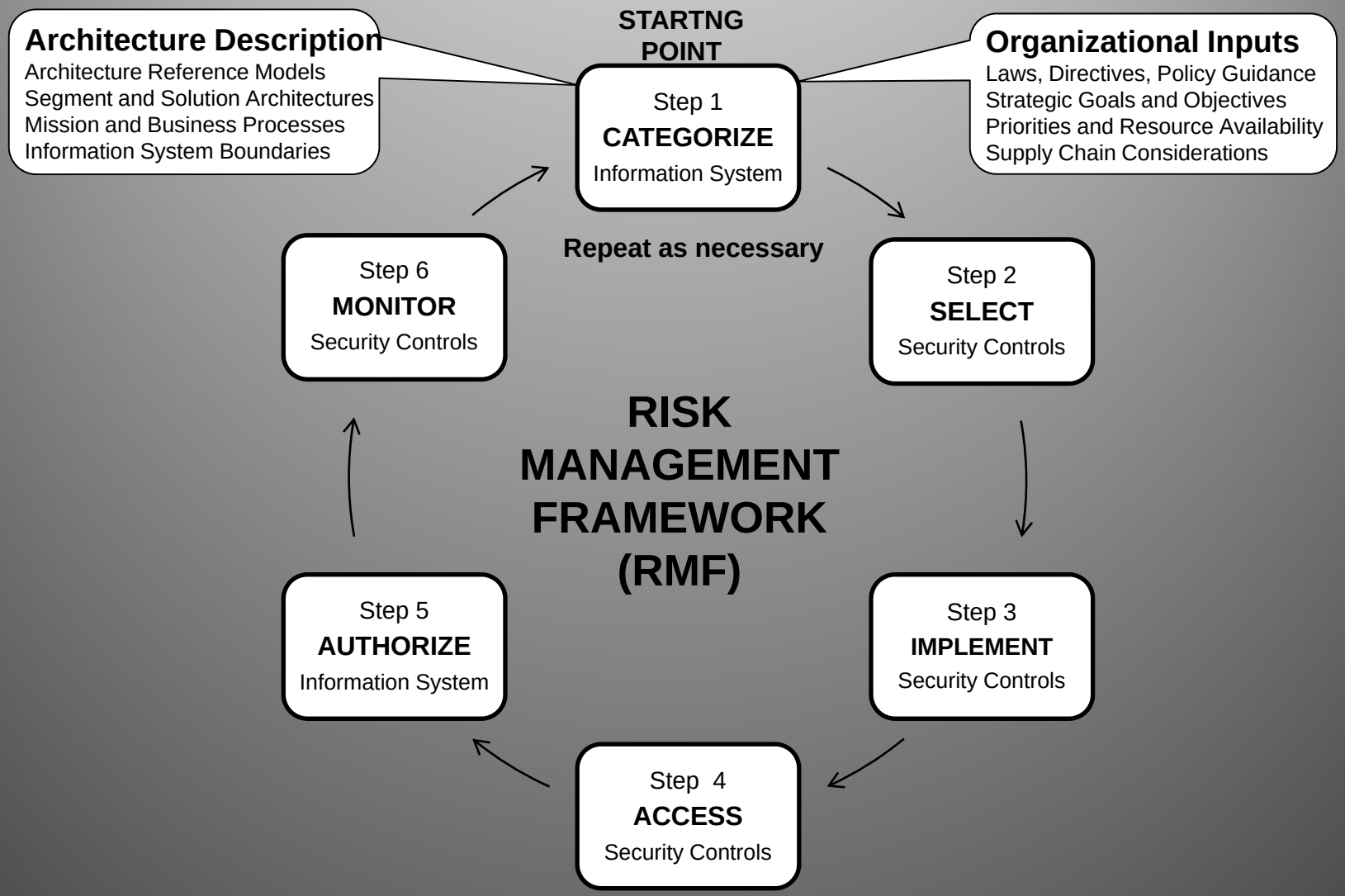
where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Managing Risk

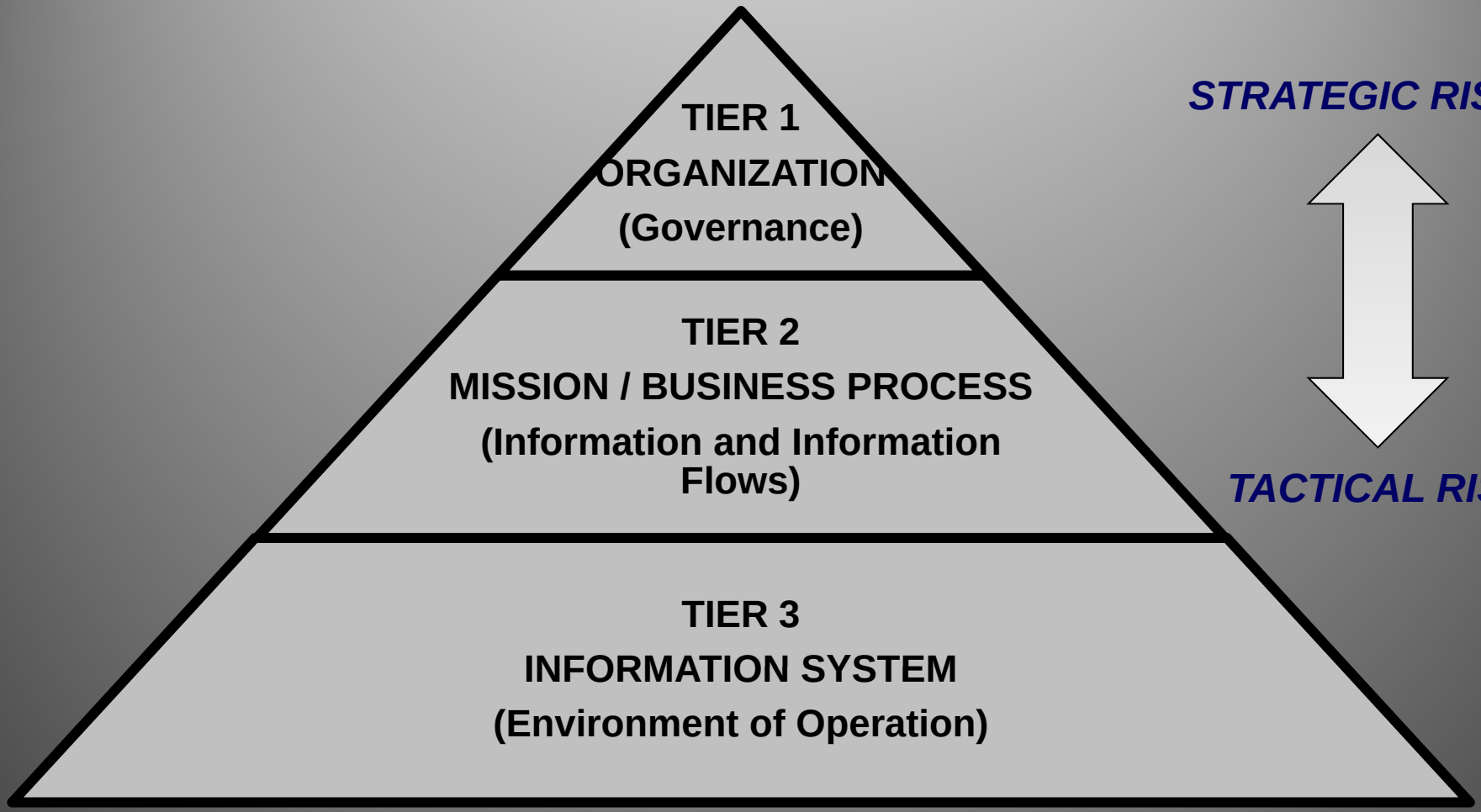
NIST System Security Lifecycle



NIST Risk Management Framework



TIERED RISK MANAGEMENT APPROACH



Step 1: Categorize

Categorize the information system and the information resident within that system based on impact.

• FIPS 199 provides a structured repeatable process to determine categories of risk based upon information types that are typically stored on Federal information systems.

• NIST SP 800-60 Revision 1 (Volume 1, Volume 2) validates the initial risk determination as identified by the FIPS 199.

Step 2: Select and Supplement

• Select an initial set of security controls from the control catalogue contained in NIST SP 800-53, as Amended for the information system based on the NIST 800-60 information types, the FIPS 199 security categorization and the minimum security requirements identified in FIPS 200;

• Apply tailoring guidance as appropriate;

• Supplement the tailored baseline security controls according to an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

Step 3: Implement

800-53 Control Family Name	Identifier	Class
Access Control	AC	Technical
Audit and Accountability	AU	Technical
Awareness and Training	AT	Operational
Security Assessment and Authorization	CA	Management
Configuration Management	CM	Operational
Contingency Planning	CP	Operational
Identification and Authentication	IA	Technical
Incident Response	IR	Operational
Maintenance	MA	Operational
Media Protection	MP	Operational
Personnel Security	PS	Operational
Physical and Environmental Protection	PE	Operational
Planning	PL	Management
Program Management	PM	Management
Risk Assessment	RA	Management
System and Communications Protection	SC	Technical
System and Information Integrity	SI	Operational
System and Services Acquisition	SA	Management

Step 4: Assess

• Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

• This is accomplished using the process defined in the NIST SP 800-53A document.

Step 5: Authorize to Operate

• This is a process that is distinct but interdependent on the results of Assessment. The decision is made by the Authorizing Official (AO) after consideration of the security assessment results, and understanding of the residual risk to the information assets and the plan of actions and milestones to mitigate the residual risk.

• The decision to authorize an information system to operate is based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.

Step 6: Continuous Monitoring

• Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

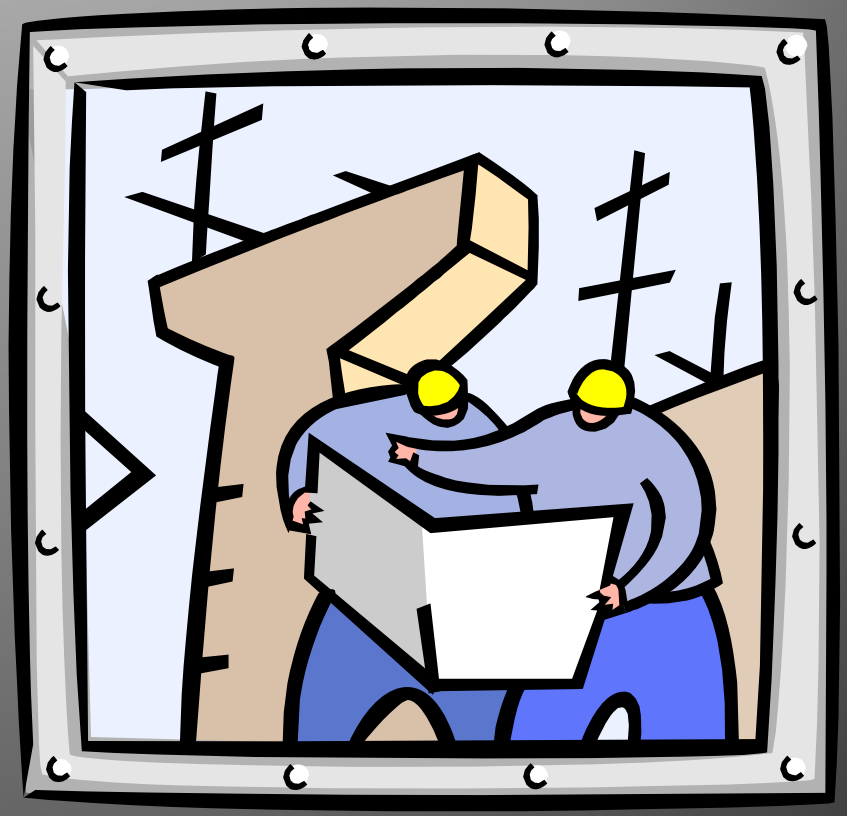
• The NIST SP 800-37 provides the process and SP 800-53A provides for the methodology for continuous monitoring of the security controls.

A&A Artifacts

- System Security Plan
- ~~Risk Assessment~~
- Security Control Assessment Plan
- Security Control Assessment Report
- Plan of Action & Milestones
- Authorization ~~Letter~~ Decision Document

Planning

- Level Of Effort based on Security Categorization
- Consider:
  - System Size and Complexity
  - Existing Controls
  - Tools
  - Available Resources
- Formal Plan

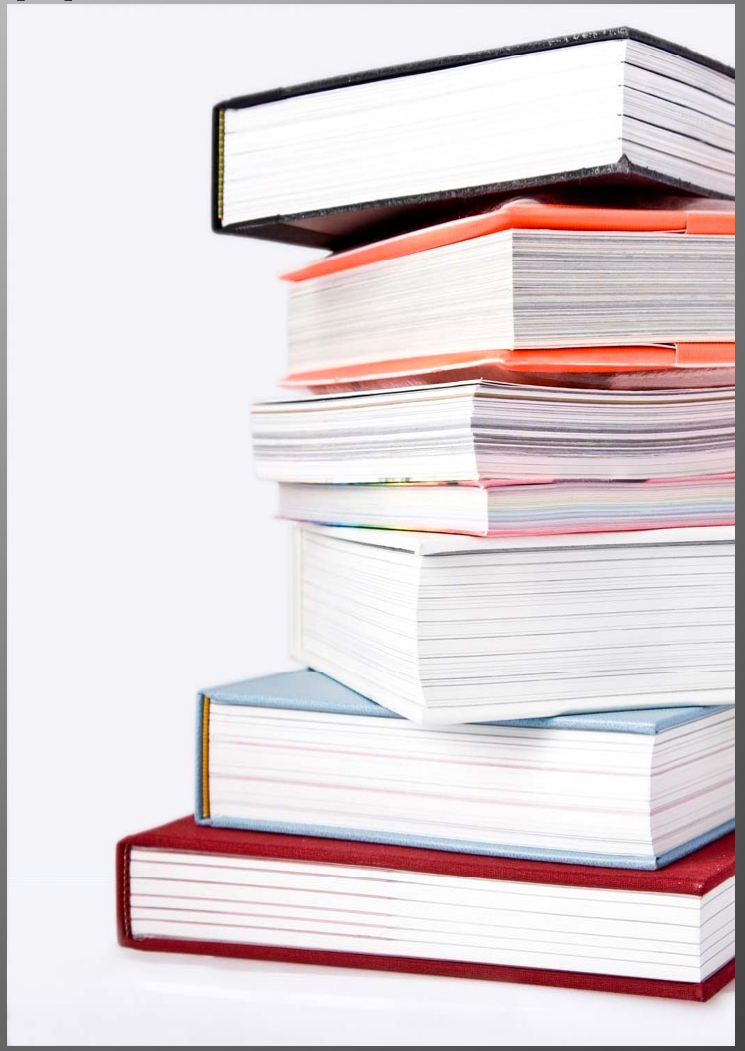


System Definition

- Direct management control
- Same function/mission
- Similar characteristics/security needs
- Same operating environment
- Boundaries

System Definition- cont.

- Mission or Management Support
- Information Types, i.e.
  - Input
  - Stored
  - Processed
  - Output
- SW and HW Assets
- Security Categorization



System Security Plan

- Reflects the strategy for protecting information contained in the system
- System Identification
- Management Controls
- Operational Controls
- Technical Controls
- Testing Methodology
- Implemented vs Planned

System Security Plan
- System Identification

- System Name/Title/Identification Number
- Responsible Organization
- Contacts
- Operational Status
- Description/Purpose
- Environment
- Interconnection/Information Sharing
- Applicable Laws/Regulations
- Security Categorization

Risk Assessment

Based on NIST SP 800-30

Step 1 — System Characterization

Step 2 — Threat Identification

Step 3 — Vulnerability Identification

Step 4 — Control Analysis

Step 5 — Likelihood Determination

Step 6 — Impact Analysis

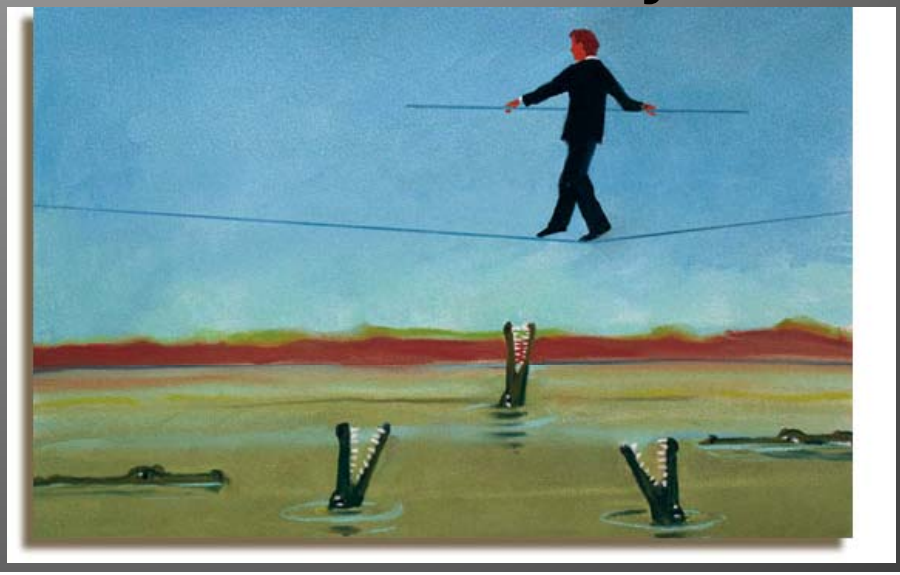
Step 7 — Risk Determination

Step 8 — Control Recommendations

Step 9 — Results Documentation

Risk Determination

- **The likelihood of a given threat-source's attempting to exploit a given vulnerability**
- **The magnitude of the impact should a threat-source successfully exercise the vulnerability**
- **The adequacy of planned or existing security controls for reducing or eliminating risk**
- **Overall level of risk for each control determined by R= (L*I)**
  - R = Risk Rating
  - L = Likelihood value
  - I = Impact



Risk Assessment Results Documentation

- Identifies Residual Risks
- Helps senior management and mission owners make decisions on priorities within a POA&M:
  - Policy, procedural, budget, and system operational and management changes
  - Allocation of resources to reduce potential losses

Security Control Assessment

- Key NIST Guidance: 800-53/53A
- Contents
  - Introduction
  - Security Control Assessment (SCA) Approach
  - SCA Objectives
  - Test System Configuration
  - Test Execution
  - Test Results
  - Observations
  - Security Findings

Continuous Monitoring
Status Reporting and Documentation

The typical reporting and documentation during the continuous monitoring phase is related to:

Critical Document Updates

- System Security Plan
- Security Assessment Report
- Plan Of Action and Milestones

Security Status Reporting –security status of and changes to the information system to the authorizing official and other appropriate organizational officials on a periodic basis.

Ongoing Risk Determination And Acceptance – Periodically review the reported security status of the information system and determine whether the risk to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable.

System Removal And Decommissioning – Implement an organizationally approved information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

RMF Roles and Responsibilities

Key People in the Process

RMF Roles and Responsibilities

- Chief Information Officer
- Authorizing Official
- Authorizing Official Designated Representative
- Chief Information Security Officer (Senior Information Security Officer)
- Information System Owner
- Information Owner/Steward
- Information System Security Officer
- Security Control Assessor
- User Representatives??
- Common Control Provider
- Head of Agency
- Risk Executive (Function)
- Information Security Architect
- Information System Security Engineer

RMF Roles and Responsibilities - Chief Information Officer

- Designates a Chief Information Security Officer for the department
- Develops and maintains InfoSec policies, procedures, and control techniques
- Trains and oversees personnel with significant responsibilities for InfoSec
- Assists senior officials concerning their security responsibilities
- Coordinates annually reporting of the effectiveness of the department InfoSec program, including progress of remedial actions, to the Agency Head

RMF Roles and Responsibilities - Authorizing Official

- A Senior Level Executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Authorization Authority
- Oversees the budget and business operations of the information system
- Approves system security requirements, system security plans, and MOA/MOUs

RMF Roles and Responsibilities

- Authorizing Official Designated Representative

- Acts on the authorizing official's behalf in coordinating necessary activities during the SLC
- Can be empowered by the authorizing official to make decisions with regard to:
  - Planning and resourcing of the RMF activities
  - Acceptance of the System Security Plan
  - Determination of risk to department operations, agency assets, and individuals
- May also be delegated to:
  - Prepare the final security authorization package
  - Obtain the authorizing official's signature on the security authorization decision letter
  - Transmit the authorization package to appropriate officials

RMF Roles and Responsibilities
- Chief Information Security Officer

- Performs the Chief Information Officer responsibilities under FISMA
- Possesses professional qualifications, including training and experience, required to administer the InfoSec program functions
- Has information security duties as that official's primary duty
- Heads an office with the mission and resources to assist in ensuring agency compliance with FISMA
- Serves as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information system security officers

RMF Roles and Responsibilities - Information System Owner

- Responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system
- Develops and maintains the System Security Plan
- Ensures the system is deployed and operated according to the agreed-upon security requirements
- Decides who has access to the information system (and with what types of privileges or access rights)

RMF Roles and Responsibilities - Information System Owner (Continued)

- Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior)
- Informs key officials of the need to conduct an assessment of the information system
- Ensures that appropriate resources are available for the assessment
- Provides the necessary system-related documentation to the certification agent

RMF Roles and Responsibilities - Information Owner

- Has statutory or operational authority for specified information
- Establishes controls for the information generation, collection, processing, dissemination, and disposal
- Establishes the rules for appropriate use and protection of the subject information (e.g., rules of behavior)
- Provide input to information system owners regarding the security requirements and controls for the information systems where the information resides
- Retains these responsibility even when the information is shared with other organizations

RMF Roles and Responsibilities - Information System Security Officer

- Ensures appropriate operational security posture is maintained for an information system or program
- Serves as the principal information system security advisor to the authorizing official, information system owner, or Chief Information Security Officer
- Typically has the detailed knowledge and expertise required to manage the information system security
- Typically assigned responsibility for the day-to-day security operations of the system

RMF Roles and Responsibilities - Assessor

- Provides an independent assessment of the System Security Plan prior to initiating security assessment activities
- Determined the extent to which the controls are:
  - implemented correctly
  - operating as intended
  - producing the desired outcome with respect to meeting the security requirements for the system
- Recommends corrective actions to reduce or eliminate vulnerabilities in the information system

RMF Roles and Responsibilities - User Representatives

- Identify mission/operational requirements
- Comply with the security requirements and security controls in the System Security Plan
- Assist in the assessment and authorization process, when needed

RMF Roles and Responsibilities - Common Control Provider

- Responsible for development, implementation, assessment, and monitoring of inherited security controls
- System Security Plan
- Proper and Independent Assessments
- POAM
- Available to applicable System Owners

RMF Roles and Responsibilities - Head of Agency

- Overall responsibility to provide security protections commensurate with risk to information and information systems
- Responsible for ensuring that:
  - ✓ InfoSec management processes are integrated with strategic and operational planning processes
  - ✓ Senior management provide InfoSec for information and information systems
  - ✓ Sufficient InfoSec training provided

RMF Roles and Responsibilities - Risk Executive (Function)

- Ensures risks for individual systems are view from an organization-wide perspective
- Ensures individual system risks are managed consistently across the organization
- Tier 1

RMF Roles and Responsibilities - Information Security Architect

- Ensures Enterprise Architecture address InfoSec requirements protecting core mission and business processes
- Liaison between enterprise architect and Information System Security Engineer

RMF Roles and Responsibilities - Information System Security Engineer

- Captures and refines InfoSec requirements
- Ensures InfoSec requirements integrated into IT component products and information systems
- Activities include security architecture, design, development, and configuration

Change Summary

- C&A => A&A (as part of RMF)
- Harmonization of CNSS, DoD, IC, and civilian processes
- System Risk => Organizational Risk
- MA, GSS => Domain, Dynamic and External Subsystems
- Application => Information System
- Resiliency
- Paperwork Exercise?
- Continuous Monitoring???

Contact Info

- Lance Kelson CISSP, CSSLP, PMP
- 202-208-5064
- lance.kelson@gmail.com
- FISSEA group on GovLoop.com

Questions ??