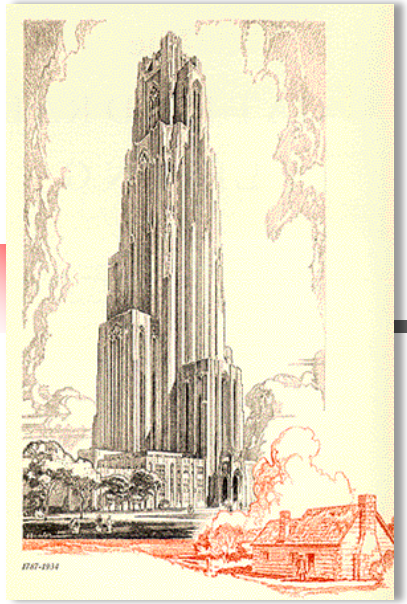
TEL2813/IS2621 Security Management



James Joshi
Associate Professor

Lecture 4 +

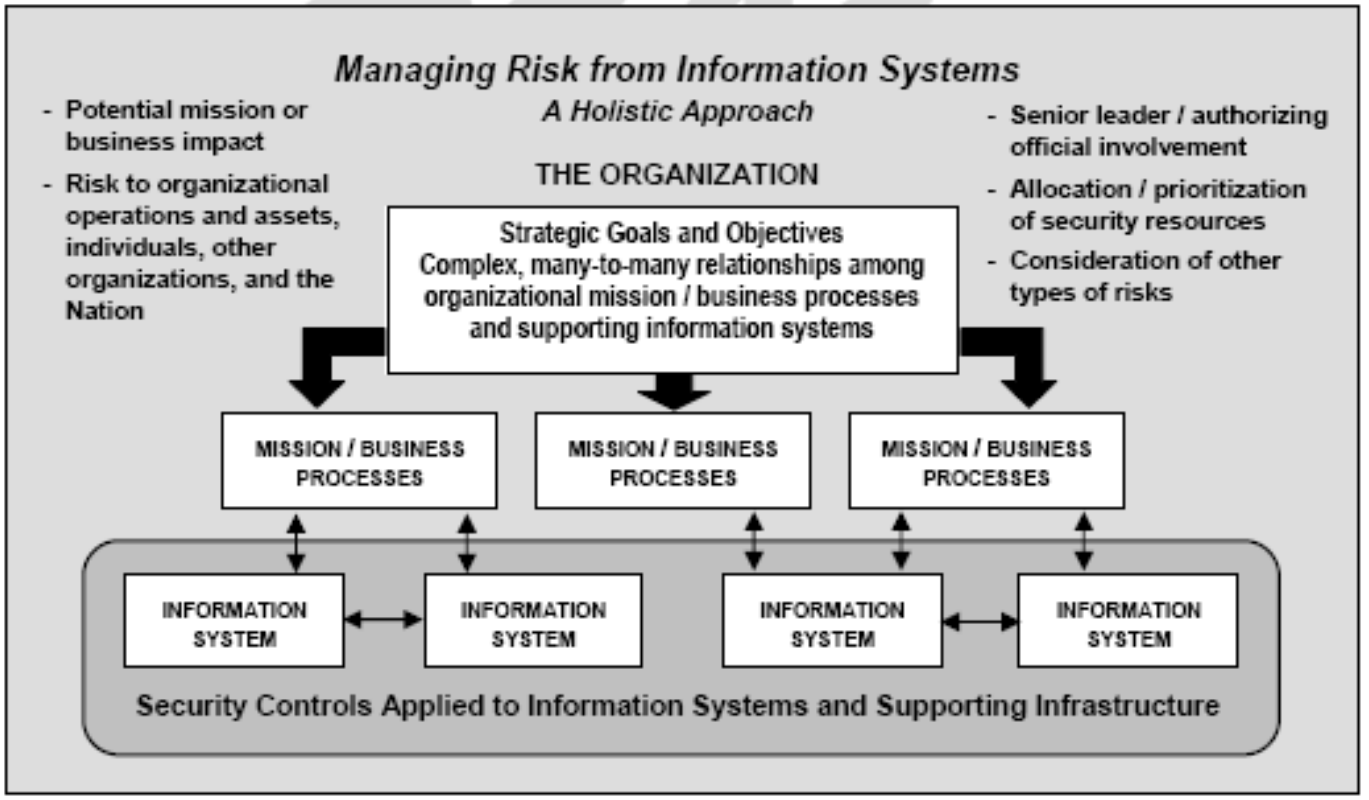
Feb 12, 2014

NIST Risk Management

Risk management concept

- Goal
  - to establish a relationship between aggregated risks from information systems and mission/business success.
- This will
  - Encourage senior leaders (including authorizing officials) to recognize the importance of management of risk
  - Help considering RM within the context of an overarching enterprise architecture and at all phases of the SDLC; and
  - Help better understand how the information security issues associated with their systems translate into organizational security concerns.

Organizational View of Risk Management



Information Security should be considered as
a *strategic capability* and an *enabler of missions/business functions*

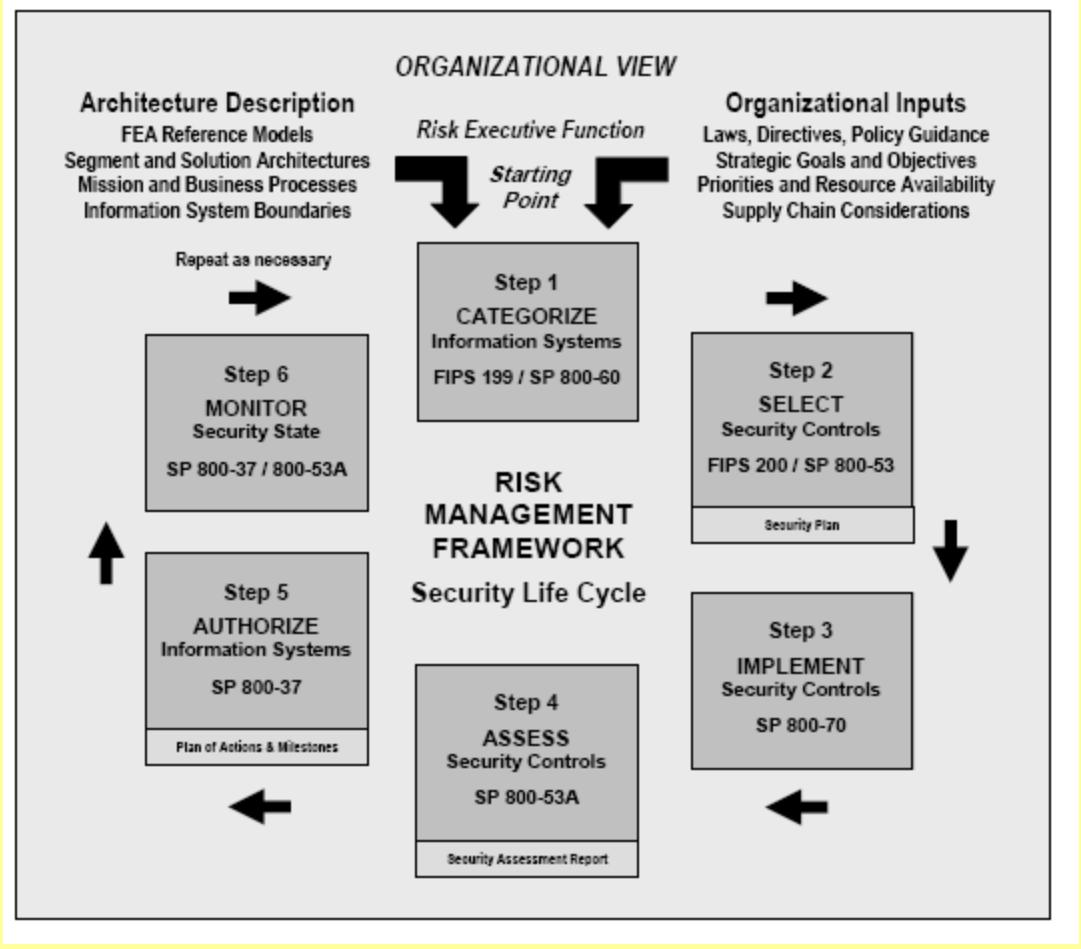
Effective Management of Risk

- Involves the following key elements:
  - Assignment of information security responsibilities to senior leaders/executives within the organization;
  - Understanding by senior leaders/executives of the degree of protection or risk mitigation that implemented security controls provide against threats;
  - Recognition and acceptance by senior leaders/executives of the risks to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of information systems; and
  - Accountability by senior leaders/executives for their risk management decisions.

Risk Management Framework

The RMF brings together other NIST documents for effective RM

NIST RMF is considerably similar to the standard ISO/IEC IT-Security Techniques-InfoSec Management systems-Requirements (published in 2005)



Some Fundamental Issues

- An Organization-wide perspective and risk executive function
- Risk-based protection strategies
- Trustworthiness of IS
- Establishing Trust relationships among organizations
- Global supply chain issues
- Strategic planning considerations

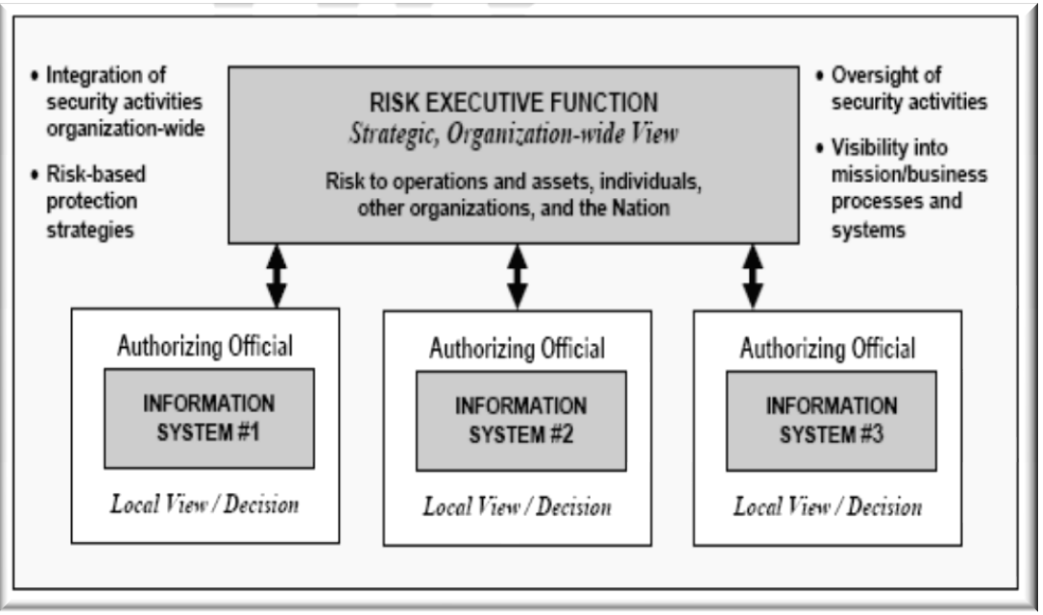
Organization-wide perspective

- Organization-wide approach
  - Facilitates prioritization of information security requirements and allocation of InforSec resources based on risks to the organization's mission/business processes;
  - Ensures InfoSec considerations are integrated into the enterprise architecture, the programming, planning, and budgeting cycles, and the acquisition, SDLCs;
  - Facilitates decisions on risk mitigation activities based on the strategic goals and objectives of the organization and organizational priorities;
  - Promotes the development and dissemination of common security policies and procedures;
  - Promotes the identification, development, implementation, and assessment of common security controls that support large segments of the organization;
  - Promotes the development of organization-wide solutions to information security problems and more consistent and cost-effective information security solutions;
  - Facilitates consolidation and streamlining of security solutions across the organization to simplify management, eliminate redundancy of protection, and improve interoperability and communication between dispersed information systems;

Risk Executive function

- Provides senior leadership input and oversight for all risk management across the organization;
- Ensures that individual authorization decisions by authorizing officials consider all factors necessary for mission and business success organization-wide;
- Provides an organization-wide forum to consider all sources of risk to organizational operations and assets, individuals, other organizations,
- Ensures that information security considerations are integrated into enterprise architectures, programming/planning/budgeting cycles, and SDLCs;
- Promotes cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Identifies the overall risk posture based on the aggregated risk from each of the information systems and supporting infrastructures
- Ensures that information security activities are coordinated with appropriate organizational entities
- Ensures that the shared responsibility for supporting organizational mission/business functions using external providers of services receives the needed visibility.

Risk Executive Function



- The intent of risk executive function
  - is to provide *visibility* into the decisions of authorizing officials and a holistic view of organizational risk.
- Authorizing officials are
  - senior leaders within the organization with mission, business, operational, and budgetary responsibilities, it is possible or likely that their authorization decisions may affect, either directly or indirectly, other parts of the organization.
- It is possible that
  - multiple authorizing officials may be responsible for information systems which collectively support a single organizational mission/business process.
- A risk executive function
  - facilitates the sharing of security-related and risk-related information among authorizing officials and other senior leaders within the organization

Risk based protection strategies

- Risk-based protection strategies require authorizing officials to:
  - Determine, with input from the risk executive function and senior agency information security officer, the appropriate balance between the risks from and the benefits of using information systems;
  - Approve the selection of security controls for information systems and the supporting infrastructure necessary to achieve this balance;
  - Take responsibility for the information security solutions agreed upon and implemented within the information systems supporting the organization's mission/business processes;
  - Acknowledge, understand, and explicitly accept the risks to organizational operations and assets, individuals, other organizations;
  - Be accountable for the results of information security-related decisions; and
  - Monitor the continued acceptability of organizational risk from information systems over time.

Trustworthiness of IS and RMF

- Trustworthiness is defined by:
  - Security functionality
  - Security assurance
- Trustworthy IS
  - Trusted to operate within a defined level of risk despite environment/human factors, and attacks
- Acceptable level of Risk guide the level of trustworthiness needed

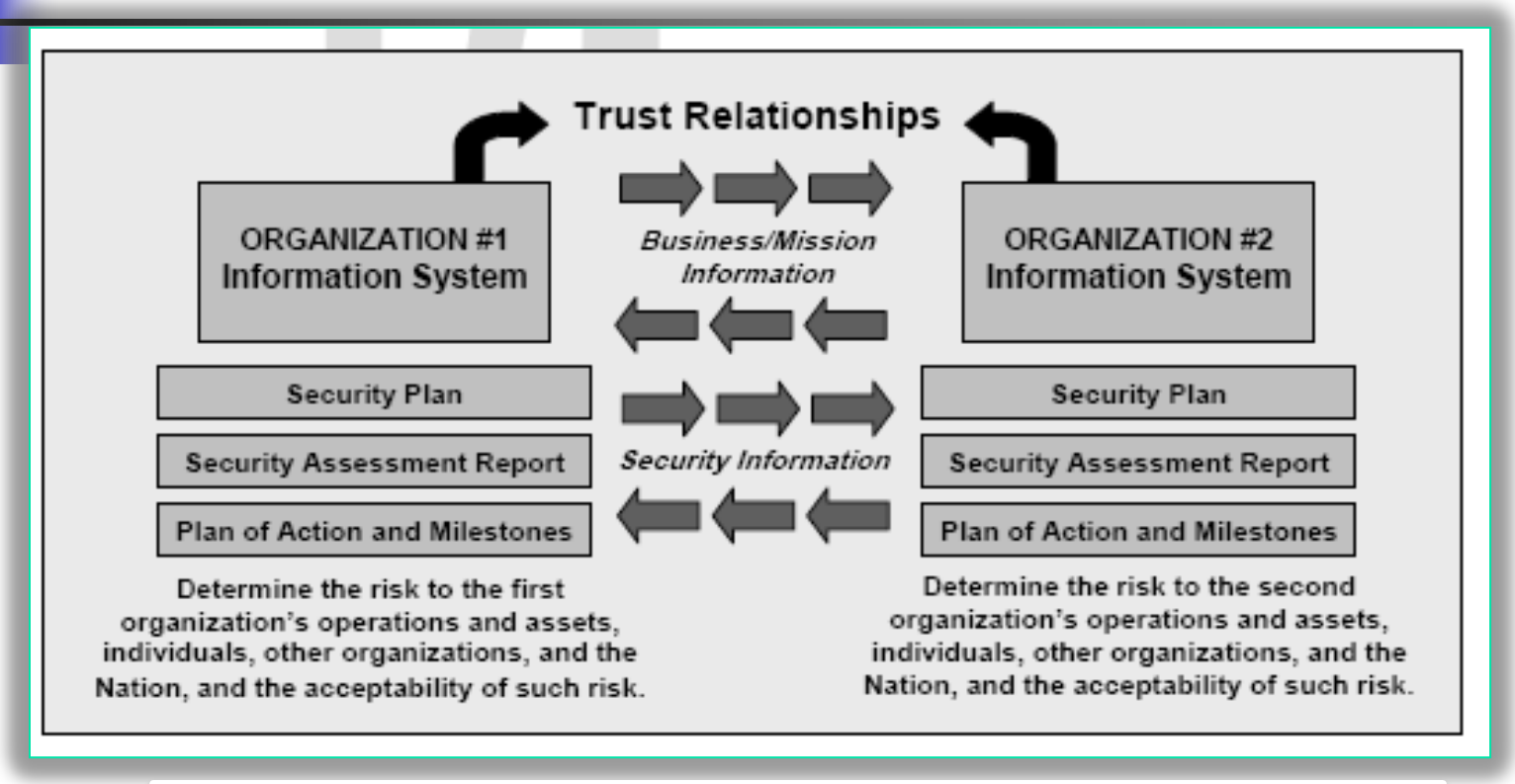
Challenges to RMF - trust relationship

- Partnerships and external IT services are becoming important
  - Trust relationships need to be carefully established
- Challenges
  - Defining the types of services/information to be provided to the organization or the types of information to be shared/exchanged in partnering arrangements;
  - Describing how the services/information are to be protected in accordance with the security requirements of the organization;
  - Obtaining the relevant information from external providers and from business partners needed to support and maintain trust and
  - Determining if the risk to organizational operations and assets, individuals, other organizations, or the Nation resulting from the use of the services or information or the participation in the partnership, is at an acceptable level

Trust relationship

- Trust among participating/cooperating partners can be established either formally or informally by:
  - Identifying the goals and objectives for the provision of services/information or information sharing;
  - Agreeing upon the risk from the operation and use of information systems associated with the provision of services/information or information sharing;
  - Agreeing upon the degree of trustworthiness needed for the information systems processing, storing, or transmitting shared information or providing services/information in order to adequately mitigate the identified risk;
  - Determining if the information systems providing services/information or involved in information sharing activities are worthy of being trusted; and
  - Providing ongoing monitoring and management oversight to ensure that the trust relationship is maintained

Trust relationship



Explicit statements of the risk to an organization's operations and assets, individuals, other organizations, and the Nation that are understood and accepted by authorizing officials (reflecting an organization's risk tolerance) are the foundation of risk-based protection and essential for establishing trust relationships among organizations.

Managing Risk from Supply Chain

- Domestic and International supply chain
  - Increasingly important to national security interests
  - Characterized by uncertainty – coupled with growing sophistication and diversity of cyber threats
- Risks include
  - The introduction of vulnerabilities into ISs when products containing malicious code and other malware are integrated into the systems;
  - Inability/difficulty in determining the trustworthiness of ISs that depend upon commercial IT products to provide many of the security controls; and
  - Inability/difficulty in determining the trustworthiness of ISs service providers (e.g., installation, operations, and maintenance) that provide many of the security controls necessary to ensure adequate security.
- Use Defense in Breadth approach to counter these risks
  - Eliminate vulnerabilities at each state of SDLC

Managing Risk from Supply Chain

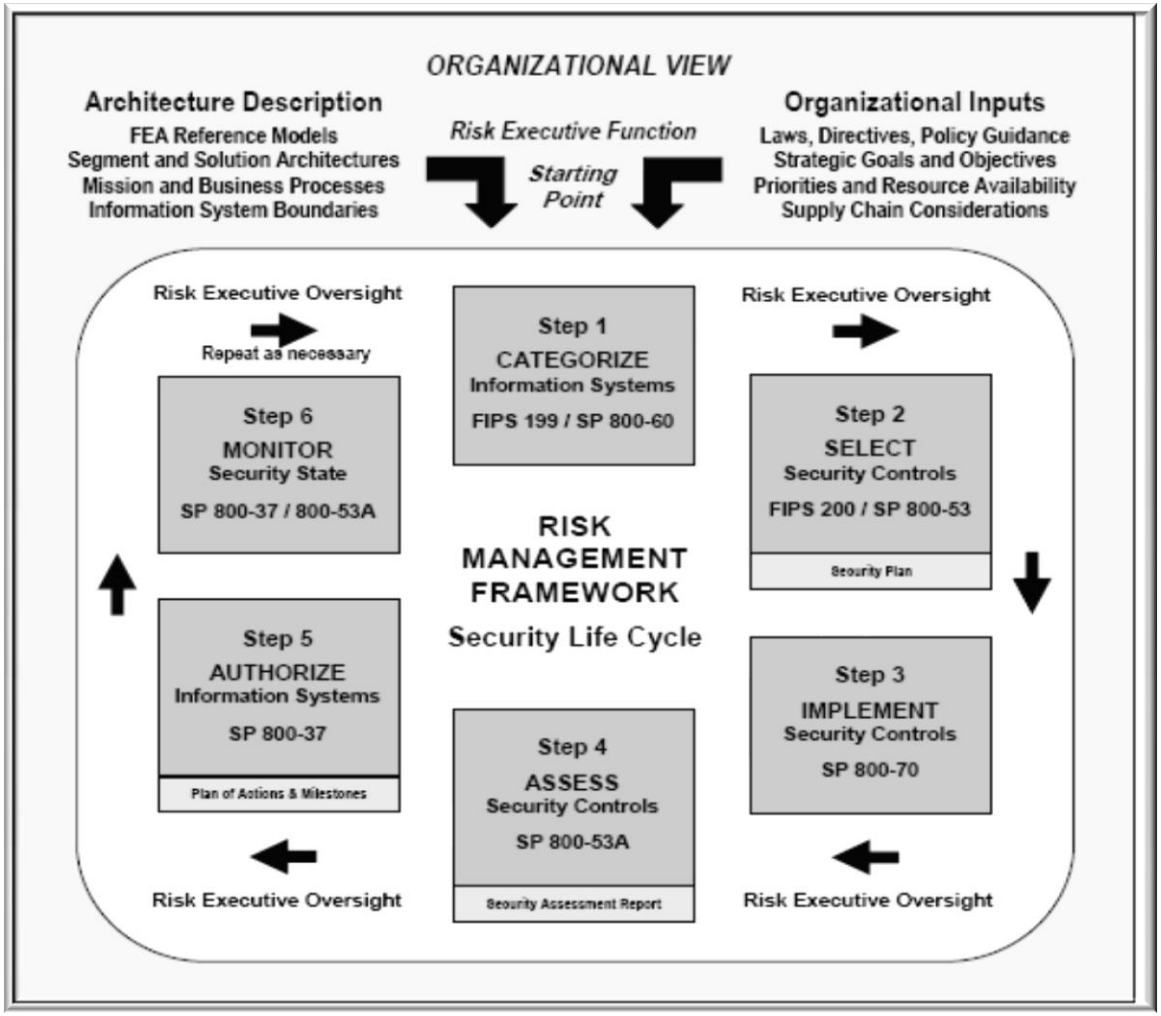
- Organizations should:
  - Know the provenance of the IT products and services provided by vendors and suppliers;
  - Use a diverse set of vendors and suppliers to minimize the adverse effects from particular item in the supply chain;
  - Seek transparency in the IT product design and development processes employed by vendors and suppliers;
  - Minimize the time between decisions to purchase IT products/services and the actual delivery date of the products/services to reduce windows of opportunity for malicious activity by adversaries;
  - Use standard configurations of to reduce probability of malicious code insertion;
  - Protect purchasing information to include the buyer's identity;
  - Implement trusted distribution processes for IT products and services;
  - Perform on-site testing of newly acquired IT products prior to widespread deployment to reduce the probability of unauthorized, covert modifications;
  - Use IT components provided by trusted vendors and suppliers;
  - Reduce the insider threat during IS upgrades or when replacing IT components by using different system administrators at different points in the layered defenses of organizations; and
  - Strictly control access to information systems for external maintenance and service providers to reduce the probability for malicious activity.

Strategic Planning Considerations

- To address growing cyber threats
  - Additional Security controls should be considered in accordance with the risk assessment
  - Strategic planning should be integral part of the protection strategy

  These include:
  - Consolidation, Simplification and Optimization of ISs (e.g., Use FEA, Secure Engg)
  - IT Use Restrictions
  - Application of a balanced set of security controls – defense-in-depth
  - Changing Architectural Configurations
  - Detection and Response to Breaches of ISs
  - Protection for Critical IS Components
  - Business Process Reengineering

Risk Management Process



Categorization (SP800-60)

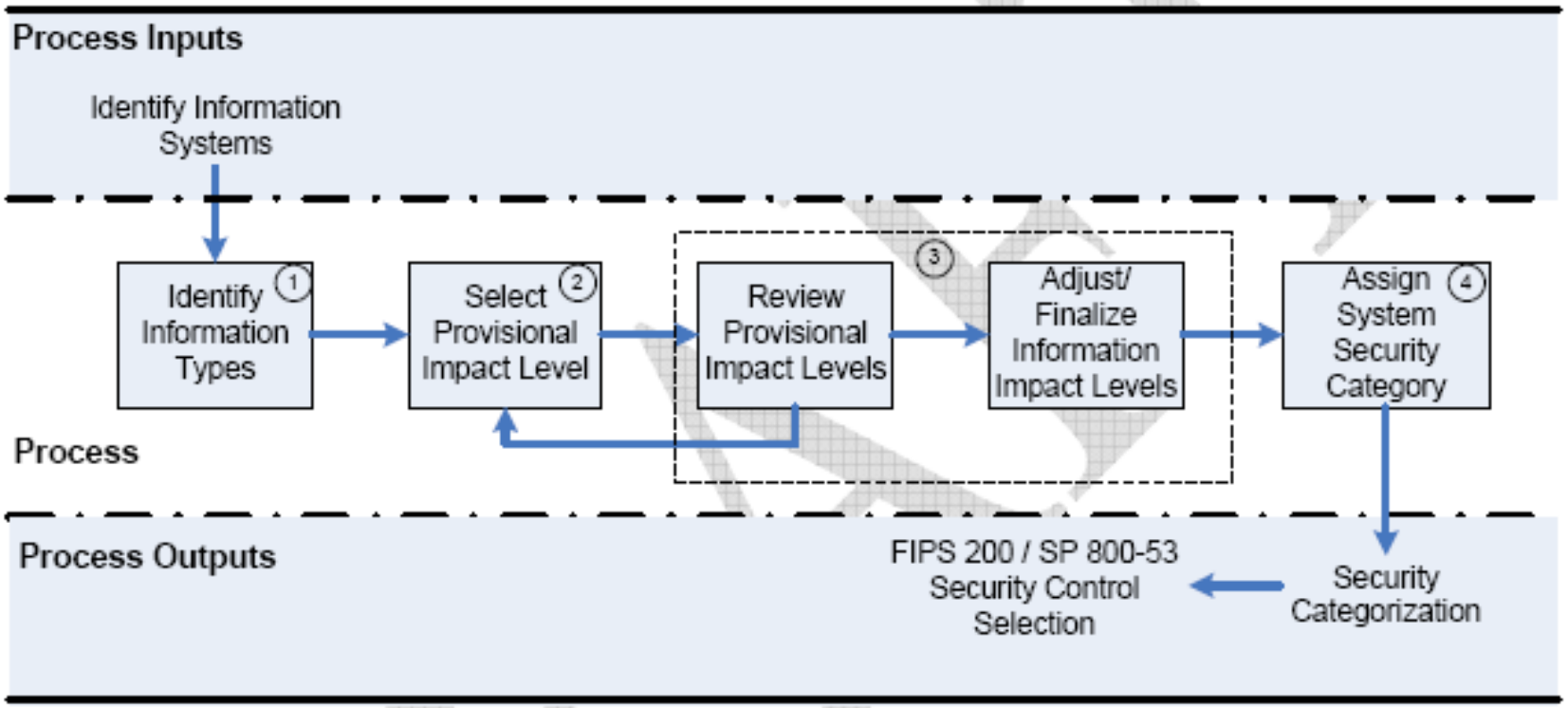


Figure 2: SP 800-60 Security Categorization Process Execution

Categorization (SP800-60)

Table 2: Mission-Based Information Types and Delivery Mechanisms[17]

Mission Areas and Information Types [Services for Citizens]

D.1 Defense & National Security
Strategic National & Theater Defense
Operational Defense
Tactical Defense

D.2 Homeland Security
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
Executive Functions of the Executive Office of the President (EOP)

D.3 Intelligence Operations
Intelligence Planning & Direction/ Needs
Intelligence Collection
Intelligence Analysis & Production
Dissemination

D.4 Disaster Management
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

D.5 International Affairs & Commerce
Foreign Affairs
International Development and Humanitarian Aid
Global Trade

D.6 Natural Resources
Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

D.7 Energy
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

D.8 Environmental Management
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

D.9 Economic Development
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
Industry Sector Income Stabilization

D.10 Community & Social Services
Homeownership Promotion
Community and Regional Development
Social Services
Postal Services

D.11 Transportation
Ground Transportation
Water Transportation
Air Transportation
Space Operations

D.12 Education
Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition

D.13 Workforce Management
Training and Employment
Labor Rights Management
Worker Safety

D.14 Health
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

D.15 Income Security
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

D.16 Law Enforcement
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement

D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

D.18 Federal Correctional Activities
Criminal Incarceration
Criminal Rehabilitation

D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

Categorization (SP800-60)

Table 2: Mission-Based Information Types and Delivery Mechanisms[12]

Services Delivery Mechanisms and Information Types [Mode of Delivery]		
D.20 Knowledge Creation & Management	**D.22 Public Goods Creation & Management**	**D.24 Credit and Insurance**
Research and Development	Manufacturing	Direct Loans
General Purpose Data and Statistics	Construction	Loan Guarantees
Advising and Consulting	Public Resources, Facility and Infrastructure Management	General Insurance
Knowledge Dissemination	Information Infrastructure Management	**D.25 Transfers to State/ Local Governments**
D.21 Regulatory Compliance & Enforcement	**D.23 Federal Financial Assistance**	Formula Grants
Inspections and Auditing	Federal Grants (Non-State)	Project/Competitive Grants
Standards Setting/Reporting Guideline Development	Direct Transfers to Individuals	Earmarked Grants
Permits and Licensing	Subsidies	State Loans
	Tax Credits	**D.26 Direct Services for Citizens**
		Military Operations
		Civilian Operations

Categorization (SP800-60)

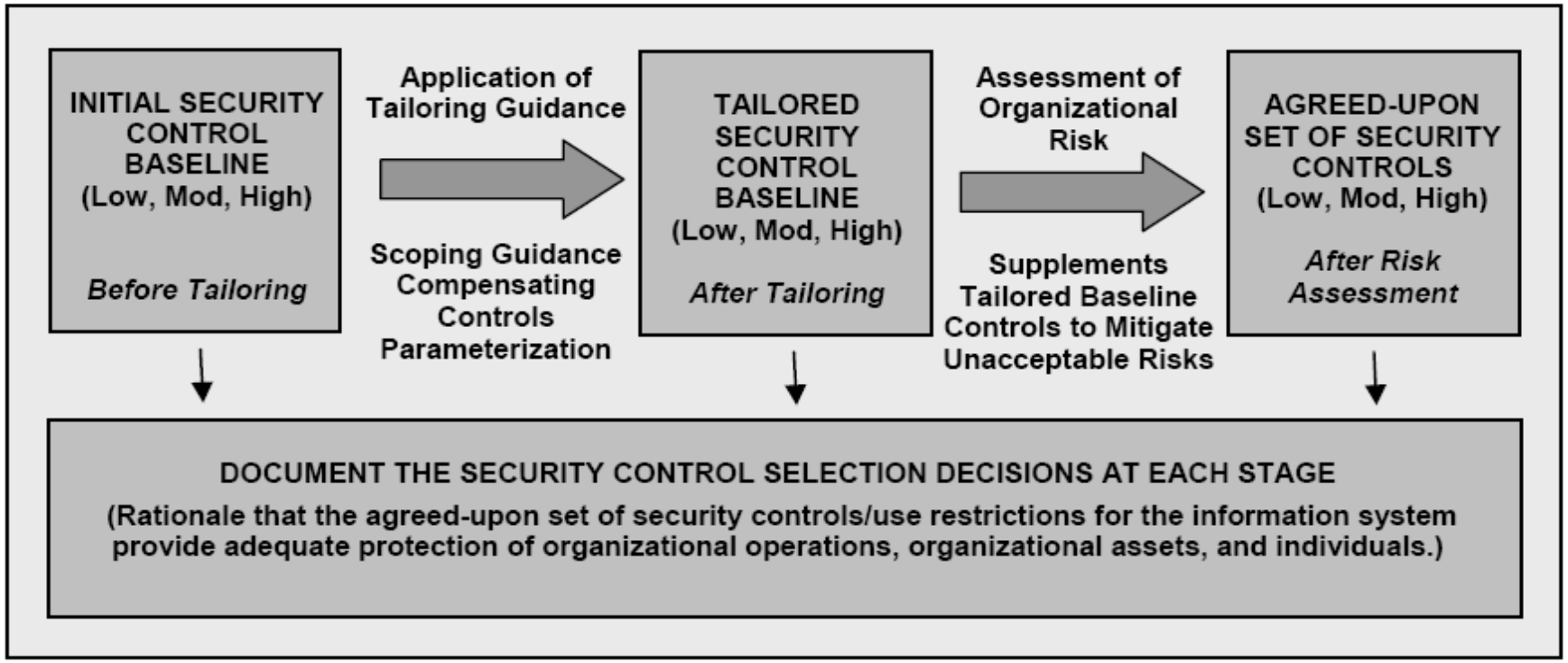
Table 5: Categorization of Federal Information and Information Systems

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

- **Key Milestone:** *Has the organization determined the criticality/sensitivity of the information and information systems needed to effectively carry out its mission/business processes and the potential adverse effects on organizational operations and assets, individuals, other organizations, and the Nation if the information and systems are not adequately protected and ultimately compromised?*

Security Control Selection Process

We discussed this in Lecture 5



- **Key Milestone:** *Has the organization selected an appropriate set of security controls to adequately mitigate the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of its information systems?*

Implementing Security Controls

- Tightly coupled with Enterprise Architecture and SDLC
- Proper allocation of security control to the appropriate components is critical
  - Defense-in-depth + defense-in-breadth
- Proper configuration settings (800-53)

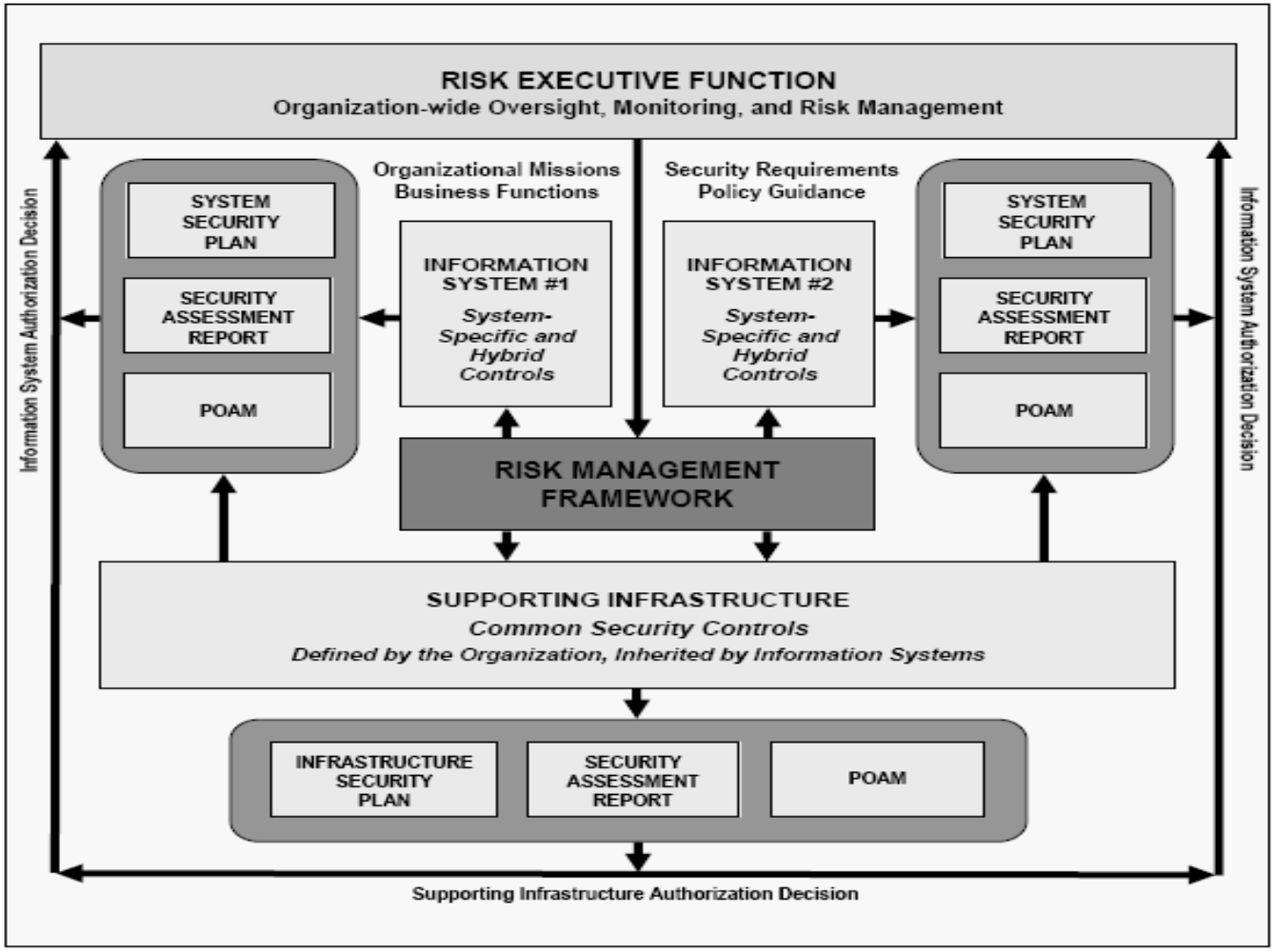
- **Key Milestone:** *Has the organization effectively implemented its organization-wide protection strategy including the agreed-upon security controls for the information and information systems supporting its mission/business processes?*

Assessing Security Controls

- Assess the collective effectiveness of the security controls
  - To [re-]evaluate accurately risks
- Security assessment reports
  - Help the organization-wide plans of actions and milestones (POAM)

- **Key Milestone:** *Has the organization assessed its organization-wide protection strategy including a determination of the effectiveness of the security controls employed within its information systems and supporting infrastructure?*

Authorizing Organizational IS (800-37)



- **Key Milestone:** *Has the organization determined and explicitly accepted the risks to its operations (i.e., mission, functions, image, reputation) and assets, individuals, other organizations (partnering or interacting with the organization), and the Nation, based on its risk mitigation decisions and implemented organization-wide protection strategy?*

Continuous Monitoring

- Effective information security programs should also include
  - comprehensive continuous monitoring programs to maintain on-going, up-to-date knowledge by senior leaders of the organization's security state and risk posture and
  - to initiate appropriate responses as needed when changes occur.
- Continuous monitoring programs achieve these objectives by:
  - Determining if the security controls in organizational ISs and supporting infrastructure continue to be effective over time as inevitable changes occur; and
  - Causing the necessary steps of the RMF to be engaged to adequately address these changes,
    - for example, re-categorizing information and information systems and responding to any changes in the FIPS 199 impact levels of the systems by appropriately adjusting security controls, and reauthorizing the systems, when required.

Continuous Monitoring

- Effective organization-wide monitoring programs include:
  - Employing strict configuration management and control processes for organizational information systems;
  - Documenting changes to the organization's information systems and supporting infrastructure;
  - Conducting security impact analyses of the changes to organizational ISs and supporting infrastructure;
  - Developing strategies for selecting and assessing subsets of security controls implemented in organizational ISs and supporting infrastructure;
  - Conducting assessments of agreed-upon subsets (and holistic assessments over an agreed-upon time period) of security controls in accordance with the priorities and frequency established by the organization; and
  - Reporting the security status of both ISs and the supporting infrastructure to appropriate organizational officials on a regular basis.

- **Key Milestone:** *Is the organization effectively monitoring the implementation of its organization-wide protection strategy on a regular basis, including an ongoing assessment of the security state of the information systems supporting its mission/business processes?*