THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

Re-aligning Security and Risk Management

Patrick D. Howard

CISO

U.S. Nuclear Regulatory Commission

Agenda

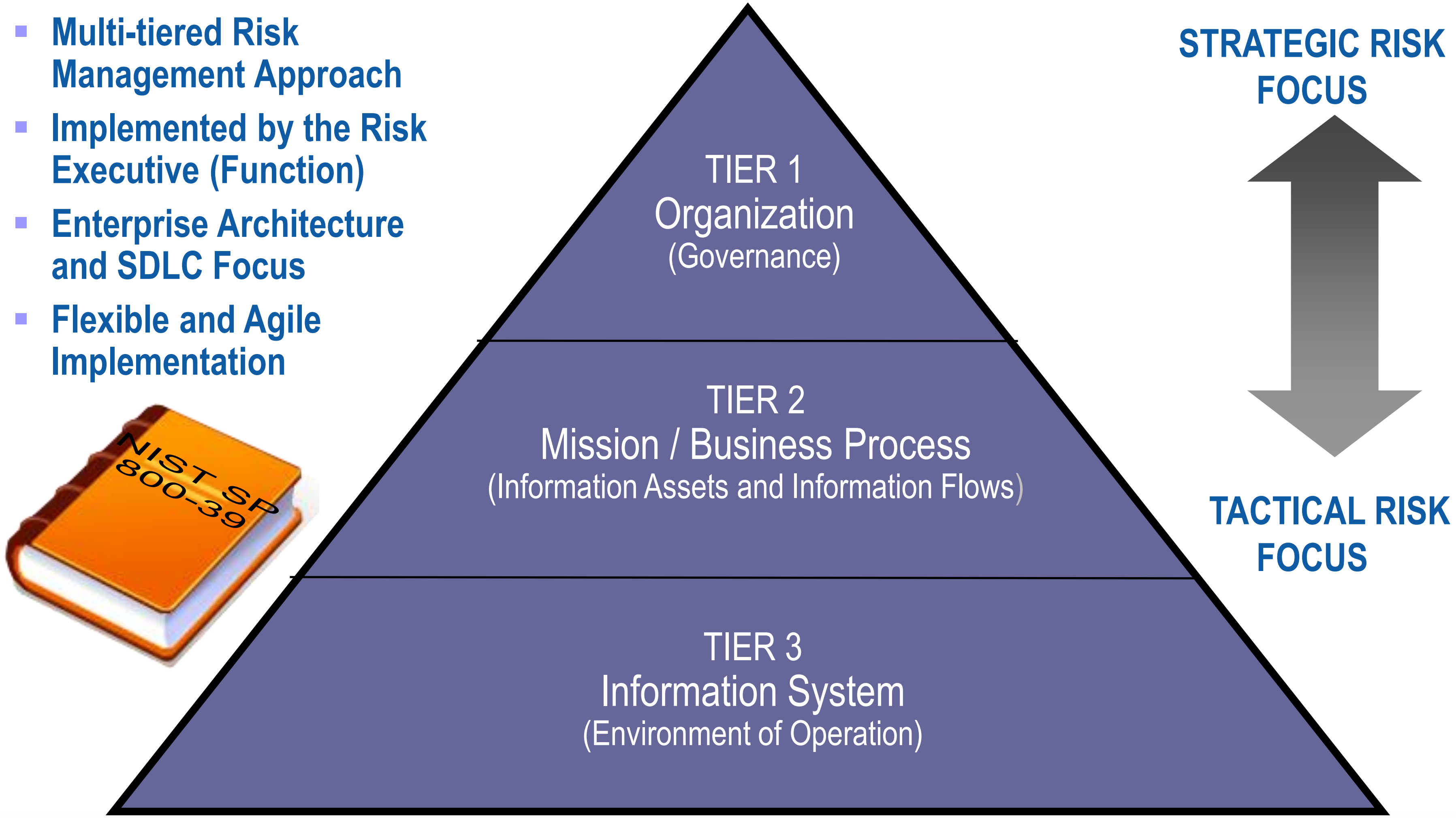
- Drivers for Enterprise Security Risk Management (ESRM)
- The New NIST Framework
- Traditional Security Risk Management vs. ESRM
- Benefits of ESRM
- Case Study: NSTS Security Categorization
- Expected Outcomes
- Implementation Status
- Summary

Drivers for Agency Wide Security Risk Management

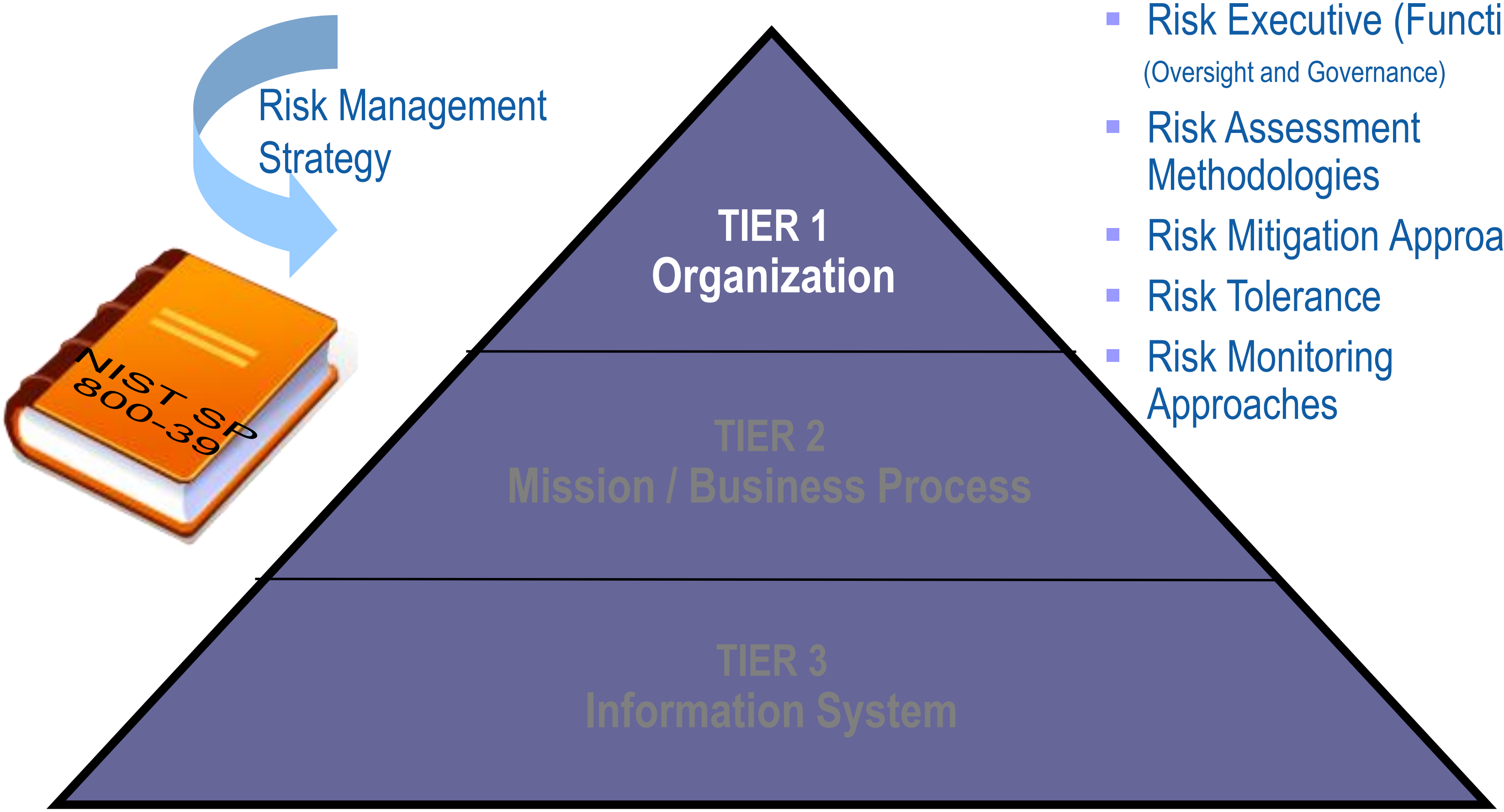
- **Federal Information Security Management Act of 2002 (FISMA)**: Requires agencies to develop, document, and implement an agency-wide information security program and emphasizes risk management for cost-effective security
- **NIST SP 800-39**: Establishes guidance for establishment of comprehensive agency level security risk management programs
- **Best Practices**: Software Engineering Institute (SEI) conducted study at the NRC in September 2007; recommended mapping risks to business needs and agency objectives in an Enterprise Risk Assessment Strategy; and recommended periodic reassessment
- **Enterprise Risk Assessment Results**: Need to address findings and recommendations of recently concluded effort.

Enterprise-Wide Risk Management Hierarchy

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive (Function)
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation

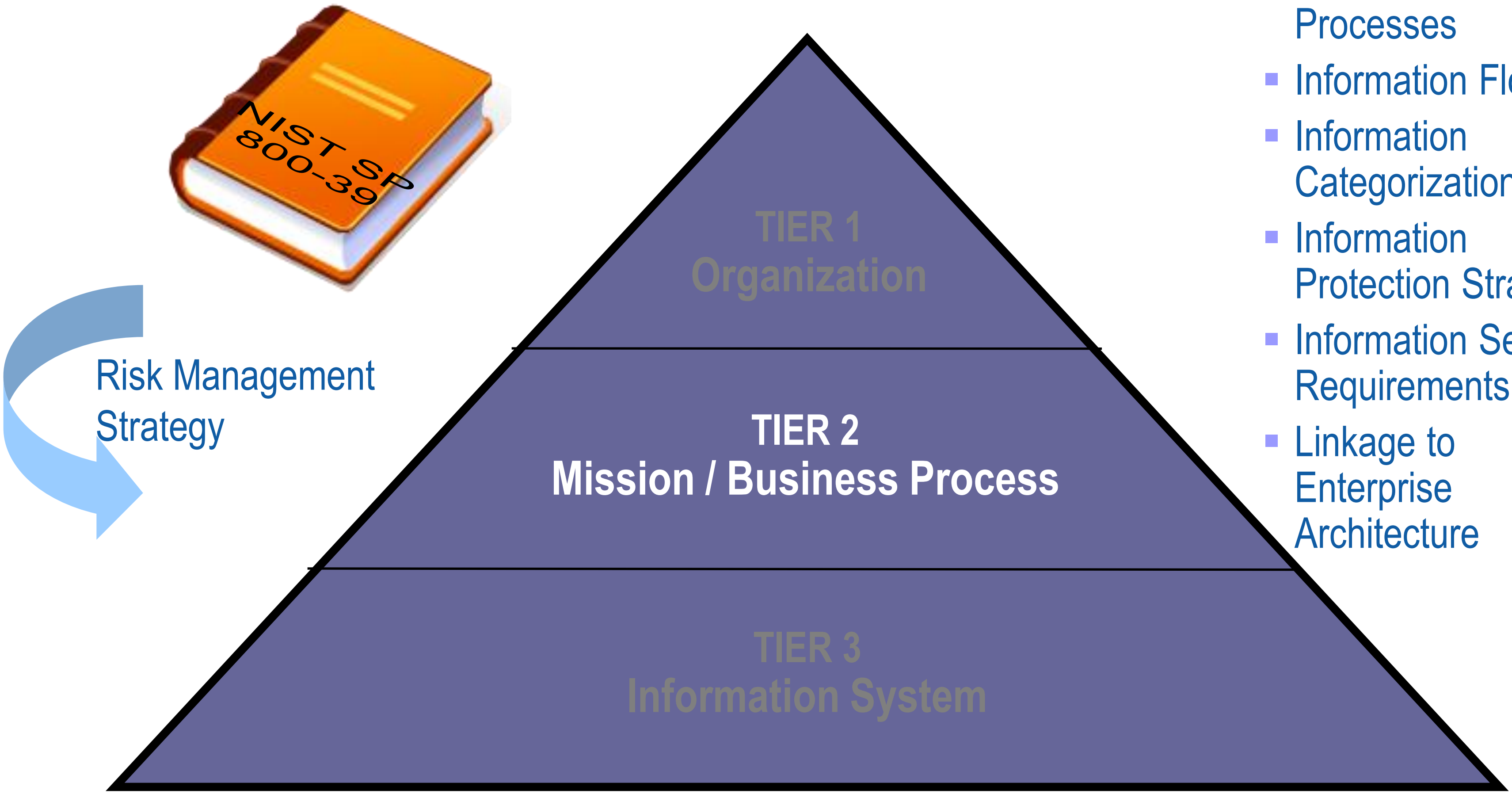


Risk Management Hierarchy



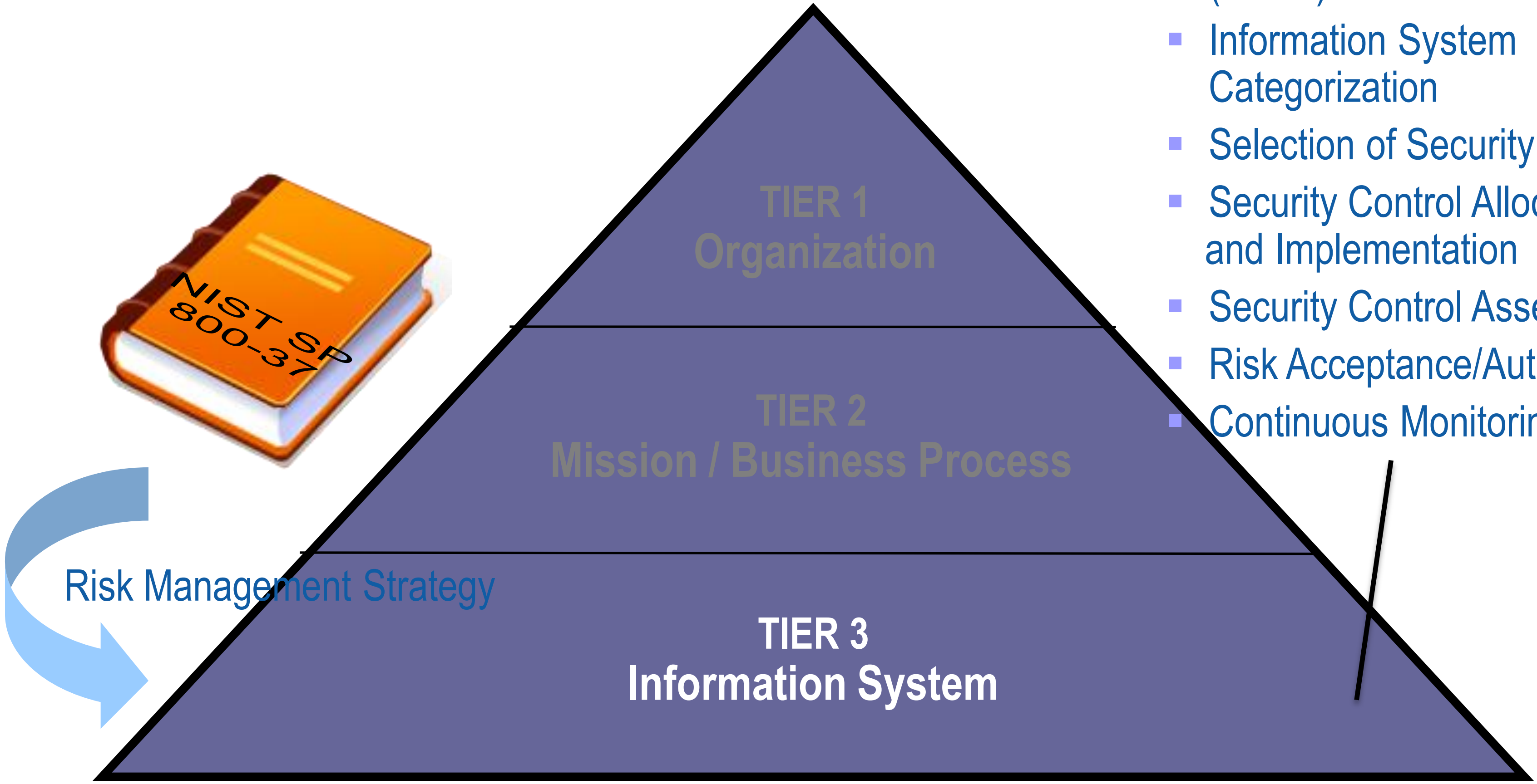
- Risk Executive (Function)
  (Oversight and Governance)
- Risk Assessment Methodologies
- Risk Mitigation Approaches
- Risk Tolerance
- Risk Monitoring Approaches

Risk Management Hierarchy



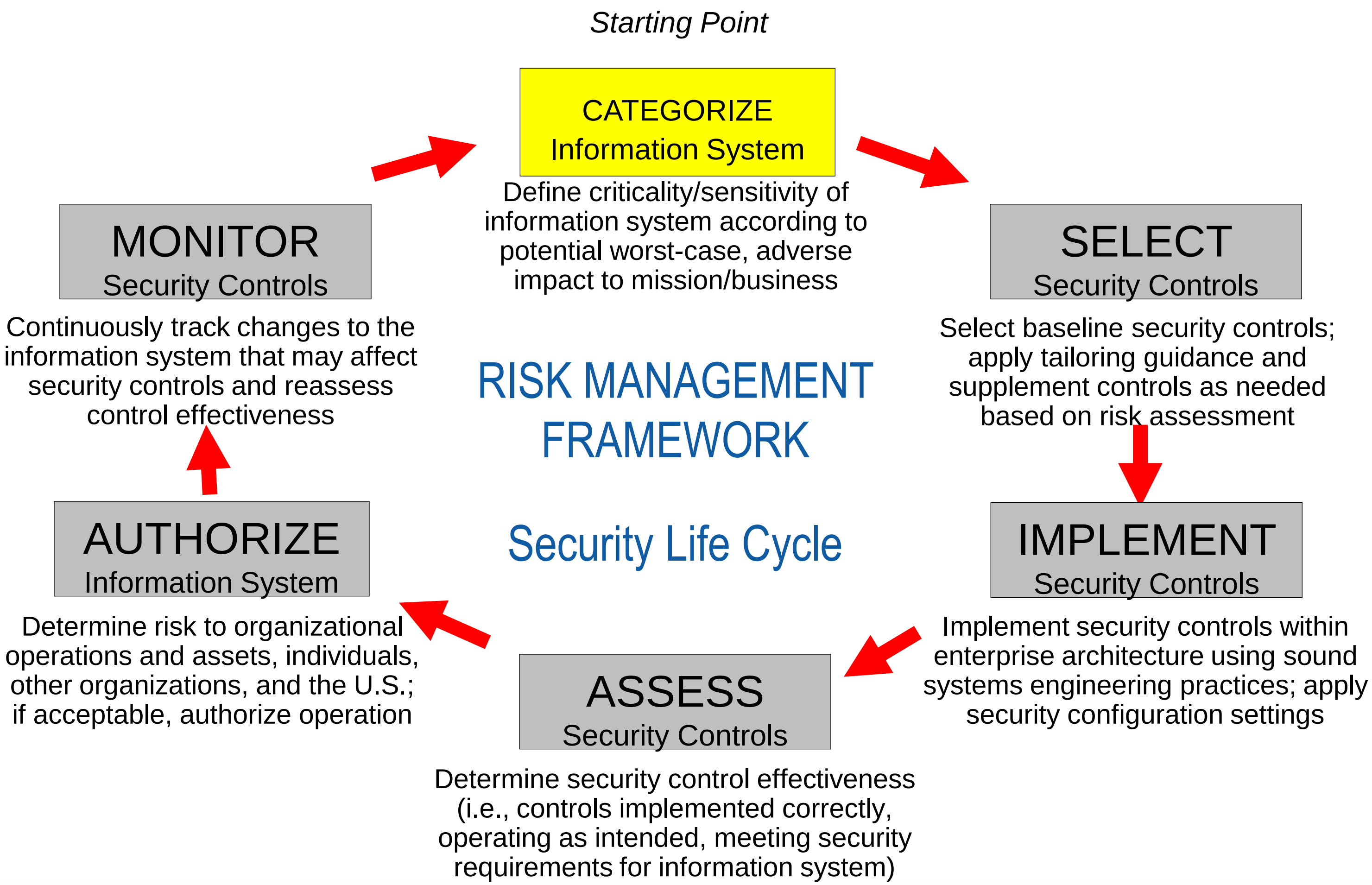
- Mission / Business Processes
- Information Flows
- Information Categorization
- Information Protection Strategy
- Information Security Requirements
- Linkage to Enterprise Architecture

Risk Management Hierarchy



- Linkage to Systems Development Life Cycle (SDLC)
- Information System Categorization
- Selection of Security Controls
- Security Control Allocation and Implementation
- Security Control Assessment
- Risk Acceptance/Authorization
- Continuous Monitoring

The New Risk Management Framework (NIST SP 800-39)



Starting Point

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings

ASSESS
Security Controls

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

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the U.S.; if acceptable, authorize operation

MONITOR
Security Controls

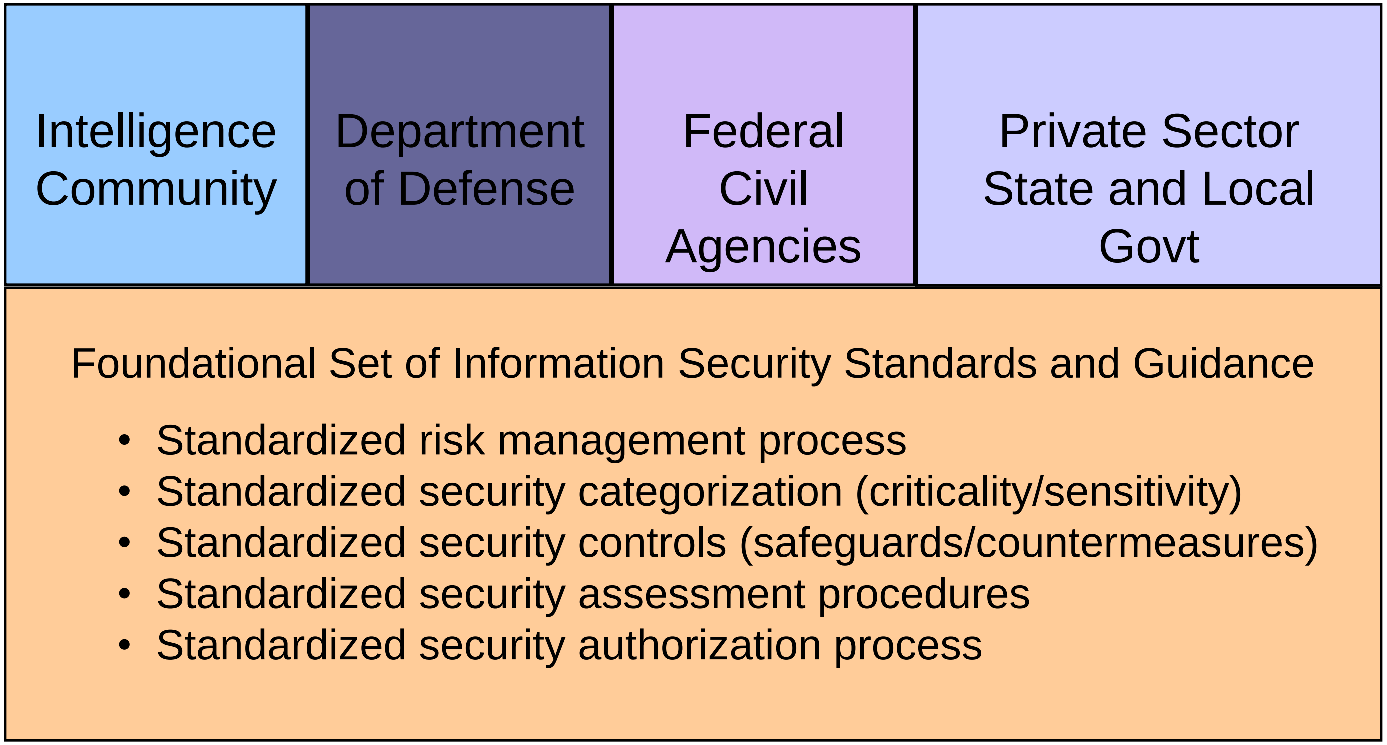
Continuously track changes to the information system that may affect security controls and reassess control effectiveness

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

A New Unified Framework For Information Security

Emphasis on Government-wide Standardization



Unique Information Security Requirements

Intelligence Community

Department of Defense

Federal Civil Agencies

Private Sector State and Local Govt

Common Information Security Requirements

Foundational Set of Information Security Standards and Guidance

- Standardized risk management process
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls (safeguards/countermeasures)
- Standardized security assessment procedures
- Standardized security authorization process

National security and non-national security information systems

Benefits of ESRM

- Enhance security risk management decision making
- Increase consistency of categorization efforts
- Improve capability for linkage of security risks to strategic goals
- Facilitate identification and application of common controls
- Bust silos – visualize risk holistically
- Improve cost effectiveness thorough assessment of risk exposure and business priorities
- Establish agency risk tolerance/appetite

Traditional vs. Enterprise Security Risk Management

- **Traditional Approach**: Focused on mitigating potential hazards or operational losses through application of security controls at the information system level

- **ESRM Approach**: Focused on strategic, financial, operational, hazard, compliance, environmental, human capital, reputation, and technology risks at the agency level

Case Study: Traditional NSTS Categorization

- Initial National Source Tracking System (NSTS) security categorization in 2006 resulted in a “High” categorization based on severe impact of risks on the following:
  - Public confidence in the NRC’s ability to fulfill its mission
  - Protection of human life
  - Security of major assets
- Requirement for Level 4 authentication resulted in lower than expected licensee use of the system
- Led to Commission review of authentication level

Case Study: ESRM-Based NSTS Categorization

- Re-categorization NSTS based on mission and business resulted in a categorization of "Moderate"
- Holistic assessment of mission and business drivers enabled NRC to balance the benefits gained from the operation and use of NSTS with the risk of operational disruptions, human and system errors, and hostile attacks
- System authentication adjusted to Level 3
- Anticipate two-fold increase in licensee use

Expected ESRM Outcomes

- Improved understanding of agency risk tolerance and information security risk posture
- Defined parameters that facilitate consistency in senior management risk management decision making
- Improved information security through awareness of business priorities and risk exposure
- Improved IT security planning and continuous monitoring
- Better integration of security requirements into the enterprise architecture and strategic plan
- Reduced costs through greater reliance on common controls and secure business solutions
- Enhanced NRC staff and IT security office alignment and coordination
- Provision of an operational risk framework to guide system owners in categorization of information and systems
- Foster consensus by creating a culture that embraces information security risk as an element of decision making

Implementation Status

- Executive management support of new approach
- Computer Security Office development of draft ESRM program plan
- Identification of resources
- Initiation of a road show to socialize concept
- Joint development of the ESRM program plan
- Full implementation by end of FY 2013

Summary

- ESRM can result in substantial improvements in an agency’s ability to protect its information
- Because of its emphasis on the interrelationship between security risk and mission requirements, active office director/staff participation in developing the NRC ERM program is essential
- Corporate buy-in and support crucial for project success

Contact Information

Patrick D. Howard, CISSP, CISM
Chief Information Security Officer
Nuclear Regulatory Commission
Rockville, Maryland

Office Phone: (301) 415-6596
Cell Phone: (240) 429-8372
Email: Patrick.Howard@NRC.gov