Next Generation Risk Management

Organization, Mission, and Information System Perspective

Industrial Control System Security Workshop

October 23, 2009

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

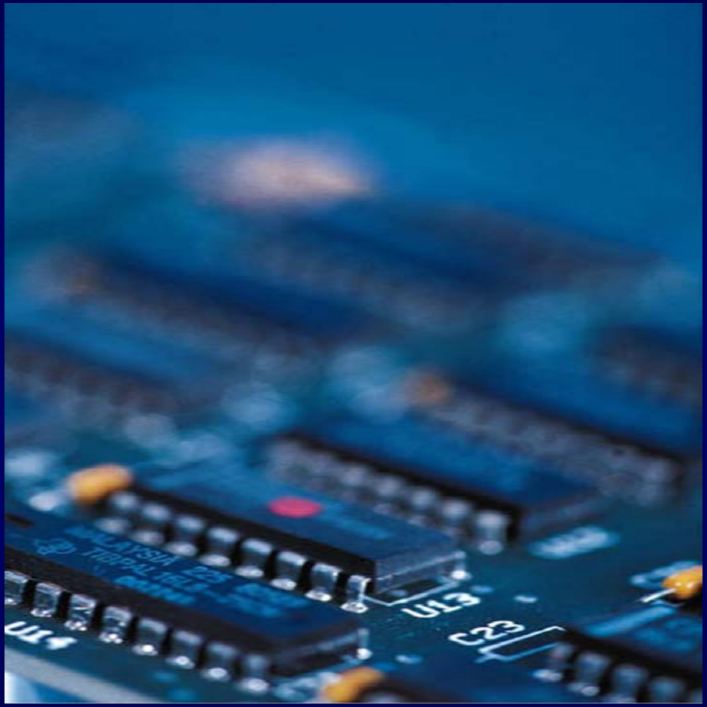
The Threat Situation

Continuing serious cyber attacks on information systems, large and small; targeting key federal, state, local, and private sector operations and assets…

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with intentions of compromising federal information systems.
- Effective deployment of malicious software causing significant exfiltration of sensitive information (including intellectual property) and potential for disruption of critical information systems/services.

Unconventional Threats to Security

Connectivity



Complexity

Asymmetry of Cyber Warfare

The weapons of choice are—

- Laptop computers, hand-held devices, cell phones.
- Sophisticated attack tools and techniques downloadable from the Internet.
- World-wide telecommunication networks including telephone networks, radio, and microwave.

Resulting in low-cost, highly destructive attack potential.

What is at Risk?

- Federal information systems supporting agencies within the federal government; state and local information systems.
- Private sector information systems supporting U.S. industry and businesses (intellectual capital).
- Information systems supporting critical infrastructures within the United States (public and private sector) including:
  - Energy (electrical, nuclear, gas and oil, dams)
  - Transportation (air, road, rail, port, waterways)
  - Public Health Systems / Emergency Services
  - Information and Telecommunications
  - Defense Industry
  - Banking and Finance
  - Postal and Shipping
  - Agriculture / Food / Water / Chemical

Strategic Initiatives

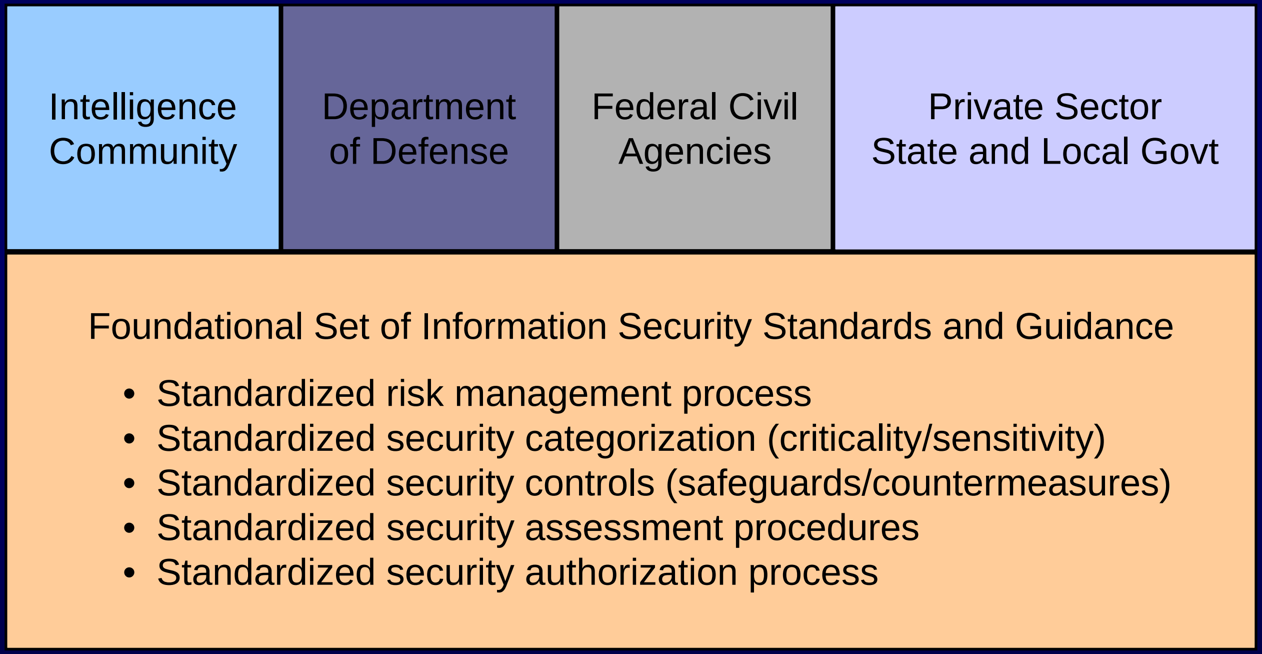
The Long-term View

- Build a unified information security framework for the federal government and support contractors.
- Integrate information security and privacy requirements into enterprise architectures.
- Work with industry to develop more secure information technology products.
- Employ systems and security engineering techniques to develop more secure (penetration-resistant) information systems.

A Unified Framework

For Information Security

The Generalized Model



***Unique* Information Security Requirements**

The "Delta"

***Common* Information Security Requirements**

Intelligence Community

Department of Defense

Federal Civil Agencies

Private Sector State and Local Govt

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

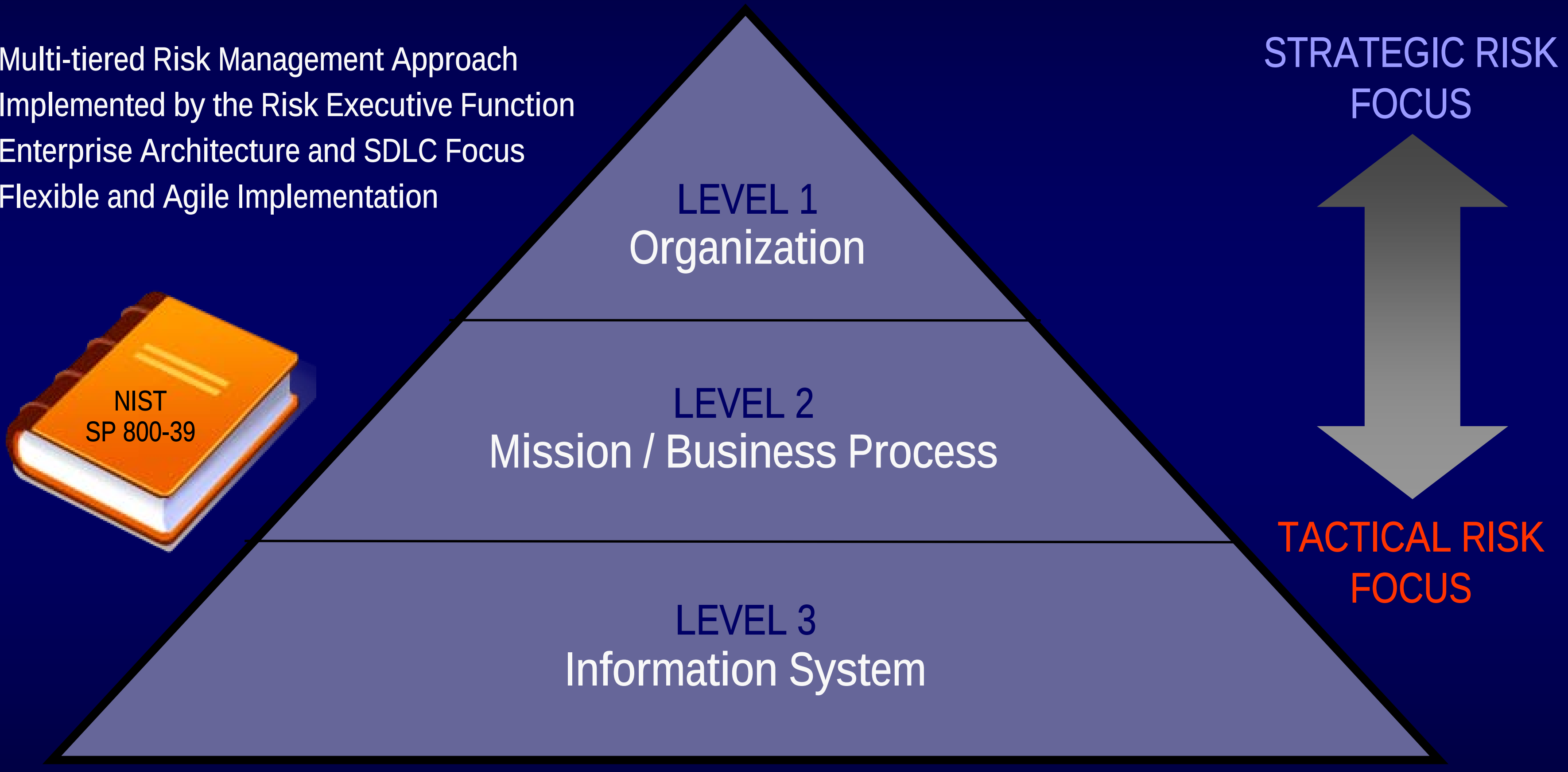
National security and non national security information systems

Risk-Based Protection

- Enterprise missions and business processes drive security requirements and associated safeguards and countermeasures for organizational information systems.
- Highly flexible implementation; recognizing diversity in missions/business processes and operational environments.
- Senior leaders take ownership of their security plans including the safeguards/countermeasures for the information systems.
- Senior leaders are both responsible and accountable for their information security decisions; understanding, acknowledging, and explicitly accepting resulting mission/business risk.

Risk Management Hierarchy

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



STRATEGIC RISK FOCUS

LEVEL 1
Organization

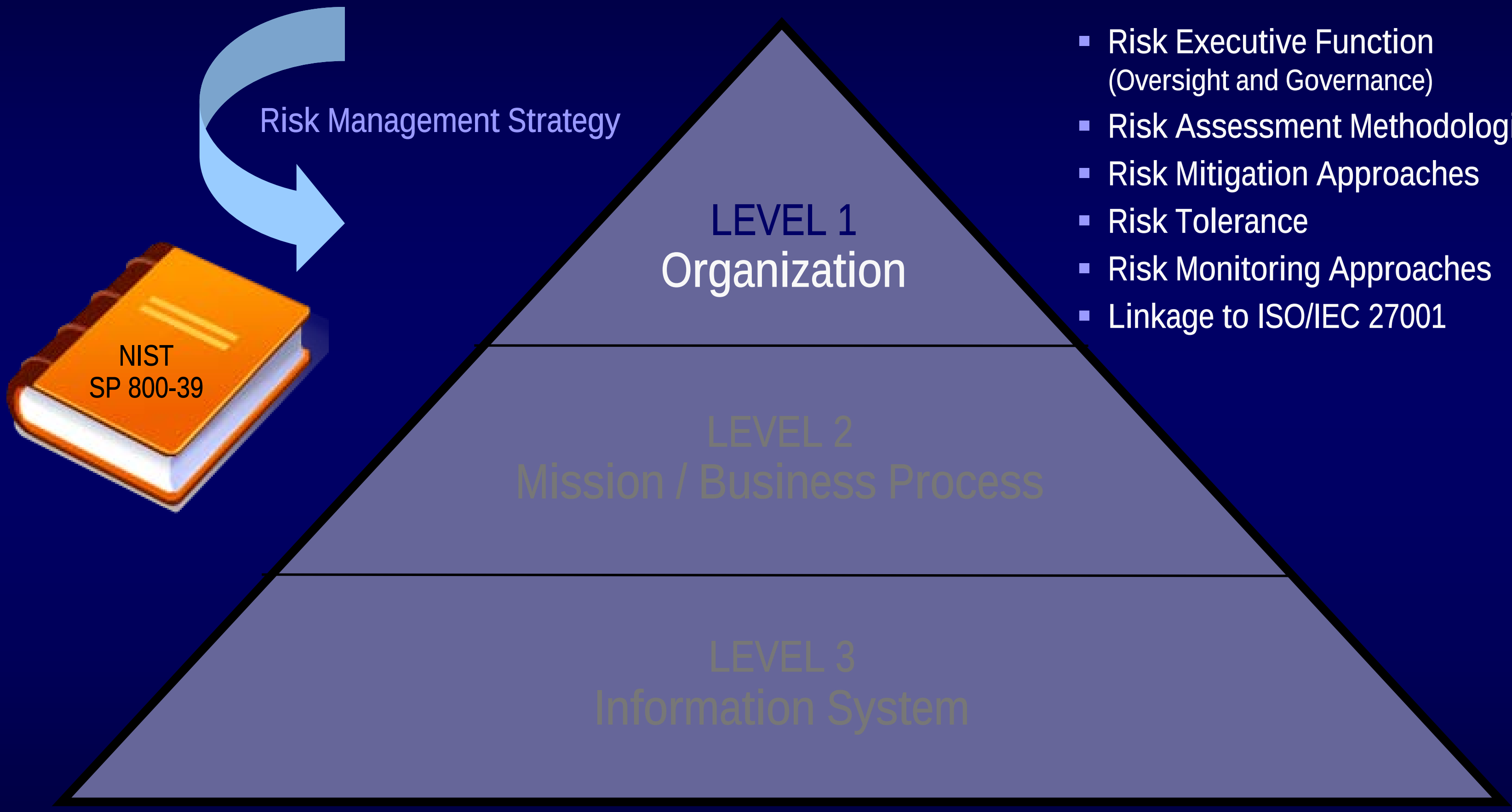
NIST
SP 800-39

LEVEL 2
Mission / Business Process

LEVEL 3
Information System

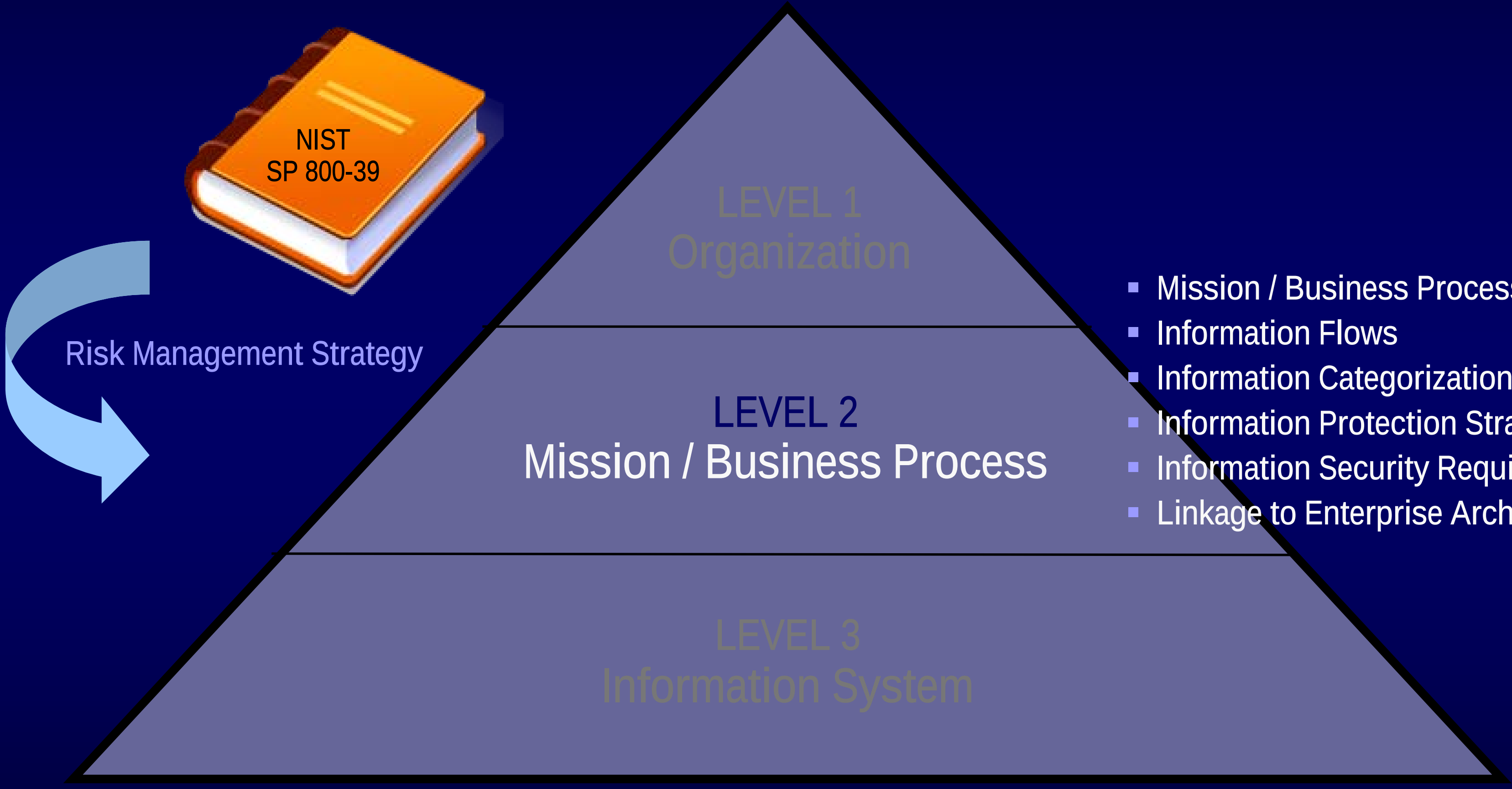
TACTICAL RISK FOCUS

Risk Management Hierarchy



- Risk Executive Function (Oversight and Governance)
- Risk Assessment Methodologies
- Risk Mitigation Approaches
- Risk Tolerance
- Risk Monitoring Approaches
- Linkage to ISO/IEC 27001

Risk Management Hierarchy



NIST
SP 800-39

Risk Management Strategy

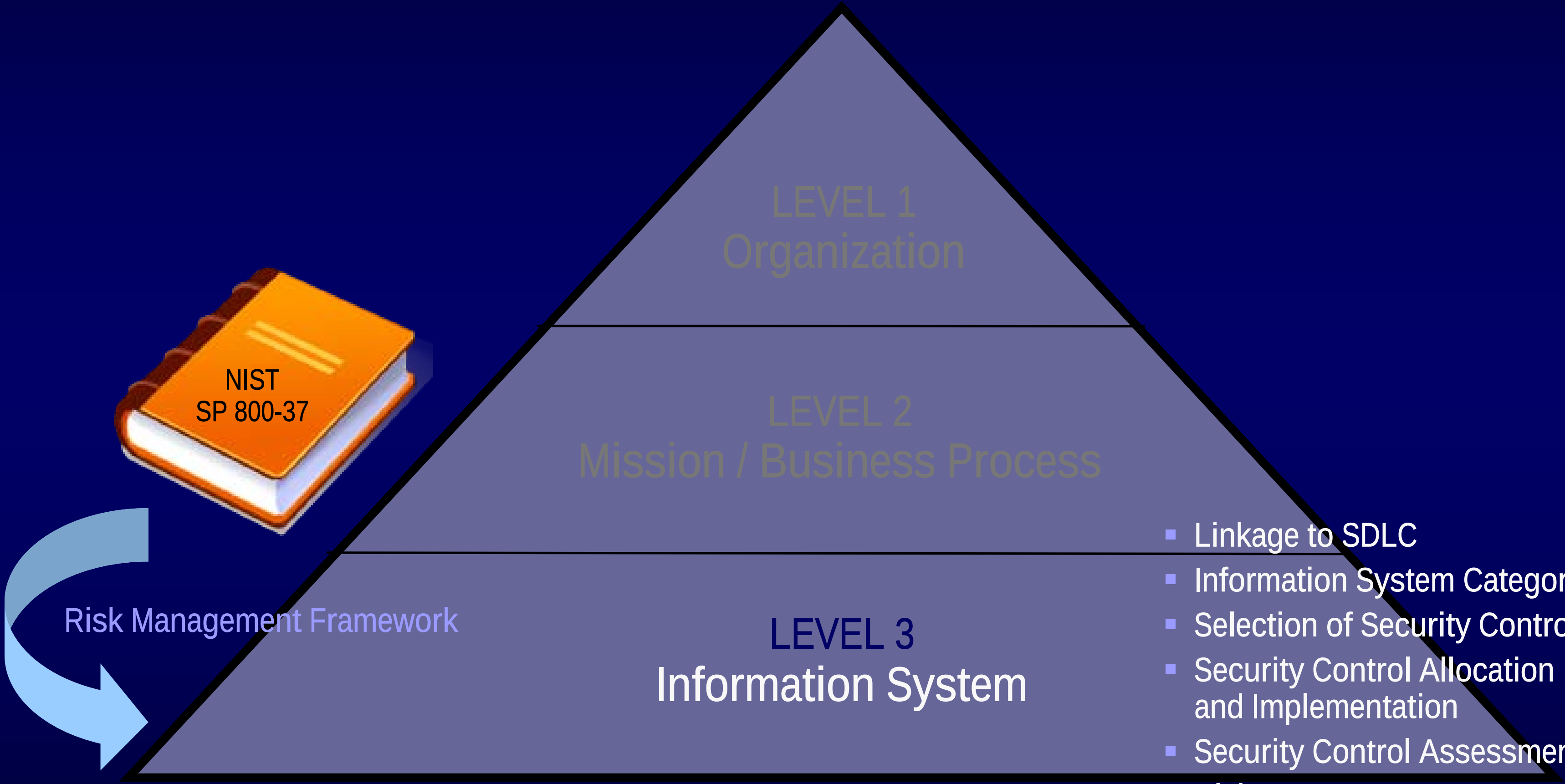
LEVEL 1
Organization

LEVEL 2
Mission / Business Process

LEVEL 3
Information System

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

Risk Management Hierarchy



LEVEL 1
Organization

LEVEL 2
Mission / Business Process

LEVEL 3
Information System

NIST
SP 800-37

Risk Management Framework

- Linkage to SDLC
- Information System Categorization
- Selection of Security Controls
- Security Control Allocation and Implementation
- Security Control Assessment
- Risk Acceptance
- Continuous Monitoring

Information Security Programs

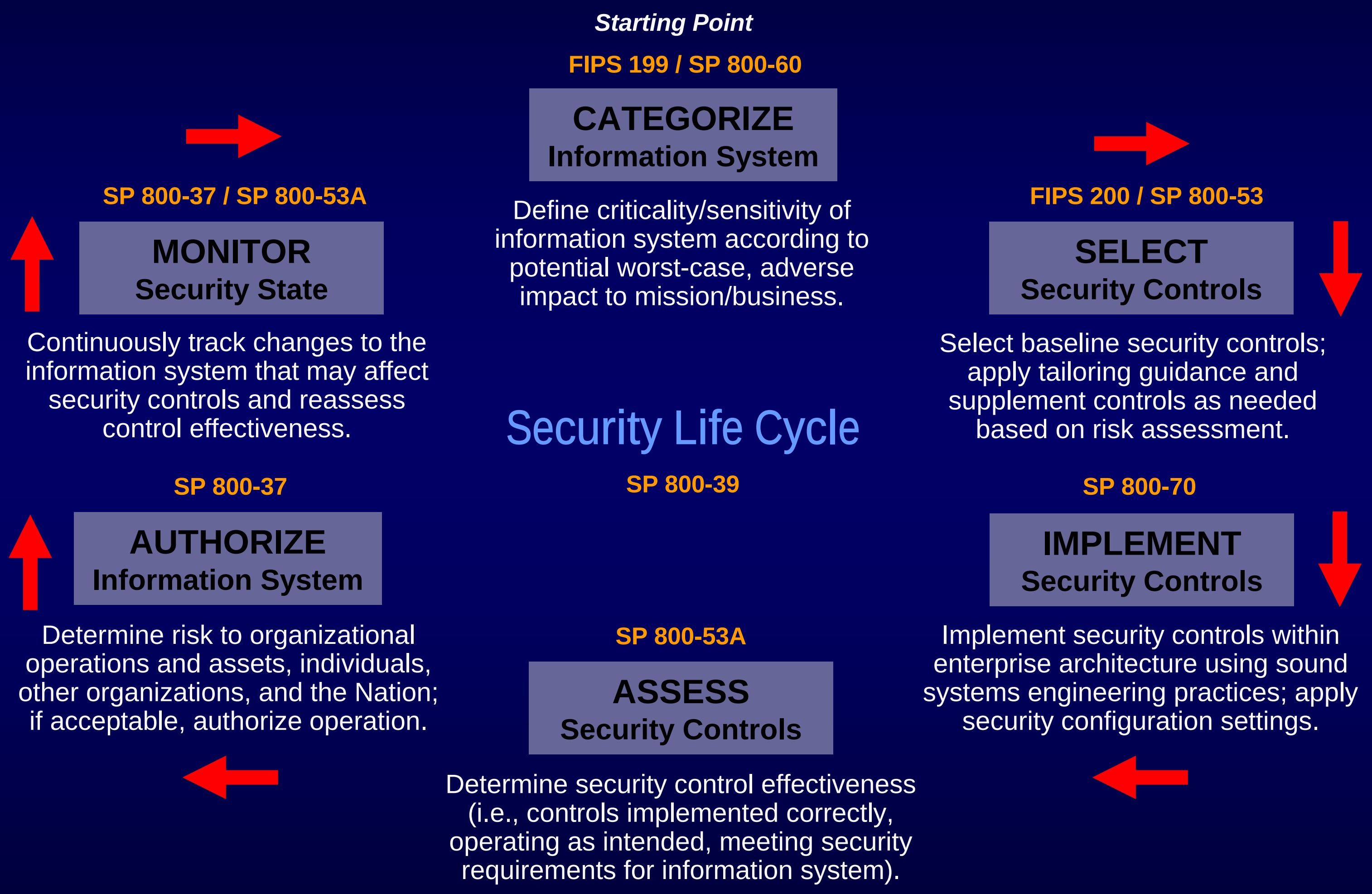
Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments and authorization
- ✓ Continuous monitoring

- ✓ 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?

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

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

FIPS 200 / SP 800-53

SELECT
Security Controls

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

SP 800-70

IMPLEMENT
Security Controls

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

SP 800-53A

ASSESS
Security Controls

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

SP 800-37

AUTHORIZE
Information System

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

SP 800-37 / SP 800-53A

MONITOR
Security State

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

Security Life Cycle

SP 800-39

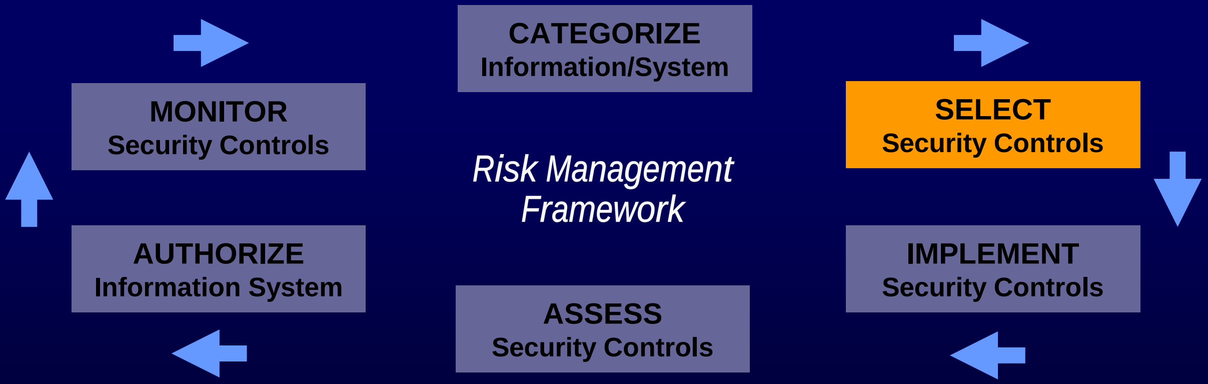
The Central Question

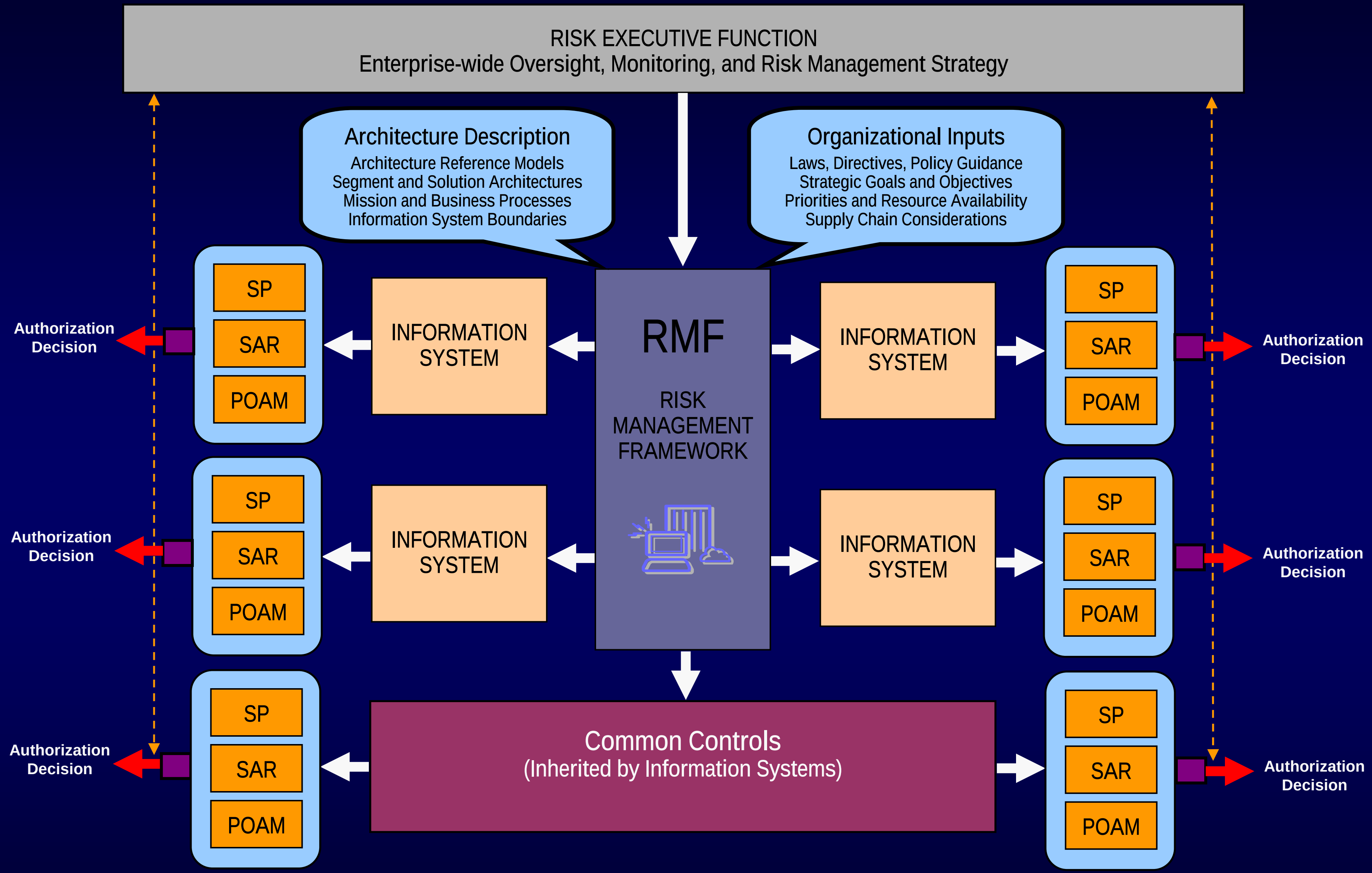
From Two Perspectives

- Security Capability Perspective
  What security capability is needed to defend against a specific class of cyber threat, avoid adverse impacts, and achieve mission success? (REQUIREMENTS DEFINITION)
- Threat Capability Perspective
  Given a certain level of security capability, what class of cyber threat can be addressed and is that capability sufficient to avoid adverse impacts and achieve mission success? (GAP ANALYSIS)

Security Control Selection

- STEP 1: Select Baseline Security Controls
  (NECESSARY TO COUNTER THREATS)
- STEP 2: Tailor Baseline Security Controls
  (NECESSARY TO COUNTER THREATS)
- STEP 3: Supplement Tailored Baseline
  (SUFFICIENT TO COUNTER THREATS)





RISK EXECUTIVE FUNCTION
Enterprise-wide Oversight, Monitoring, and Risk Management Strategy

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

RMF

RISK MANAGEMENT FRAMEWORK

INFORMATION SYSTEM

INFORMATION SYSTEM

INFORMATION SYSTEM

INFORMATION SYSTEM

Common Controls
(Inherited by Information Systems)

SP

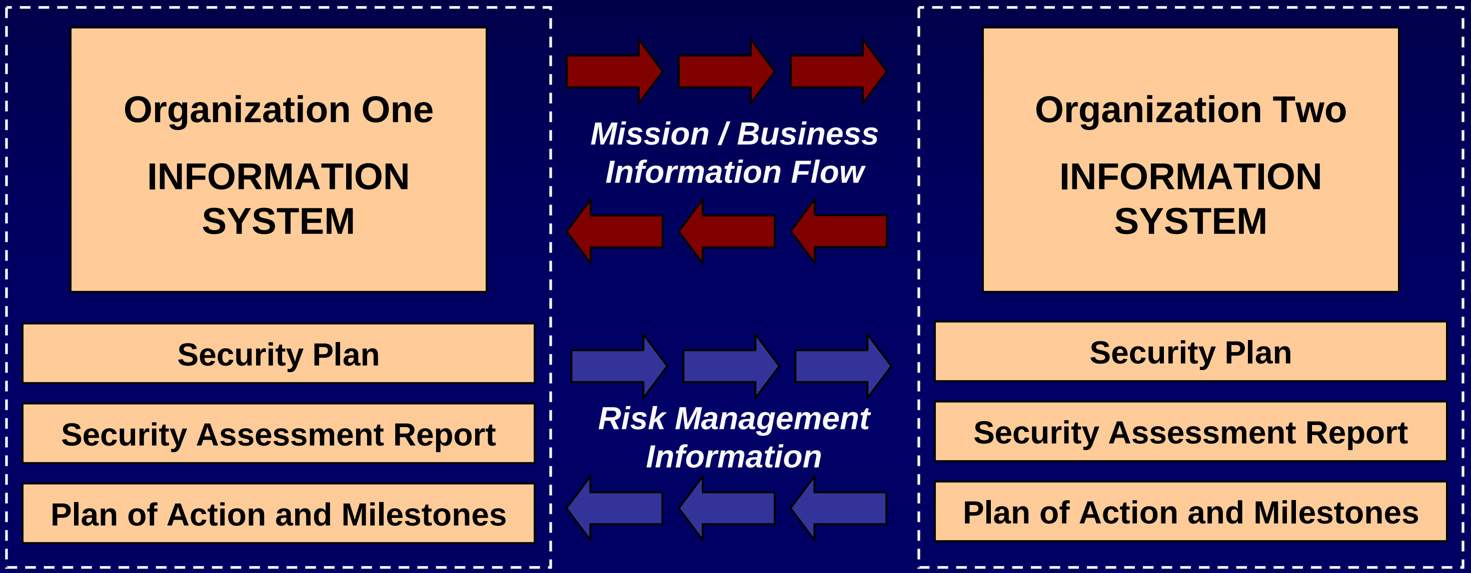
SAR

POAM

Authorization Decision

SP: Security Plan
SAR: Security Assessment Report
POAM: Plan of Action and Milestones

Trust and Reciprocity



Organization One

INFORMATION SYSTEM

Security Plan

Security Assessment Report

Plan of Action and Milestones

Mission / Business Information Flow

Risk Management Information

Organization Two

INFORMATION SYSTEM

Security Plan

Security Assessment Report

Plan of Action and Milestones

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

The objective is to achieve transparency of prospective partner's information security programs and processes…establishing trust relationships based on common, shared risk management principles.

Key Risk Management Publication

- NIST Special Publication 800-53, Revision 3
  Recommended Security Controls for Federal Information Systems and Organizations

  August 2009

  - Updating all material from NIST Special Publication 800-53, Revision 2
  - Incorporating security controls from Draft CNSS Instruction 1253
  - Incorporating new security controls for advanced cyber threats
  - Incorporating information security program-level controls
  - Incorporating threat appendix for cyber preparedness
    (Separately vetted and added to SP 800-53, Revision 3 when completed)

Key Risk Management Publication

- NIST Special Publication 800-37, Revision 1
  Guide for Applying the Risk Management Framework to Federal Information Systems

  Projected: December 2009

  - Incorporating comments from Initial Public Draft
  - Implementing guideline for Risk Management Framework
  - Transforming previous certification and accreditation process
  - Integrating Risk Management Framework into the SDLC
  - Greater emphasis on ongoing monitoring of information system security state
  - Ongoing security authorizations informed by risk executive function
  - Greater accountability and assurances for common (inherited) controls
  - Increased use of automated support tools

Key Risk Management Publication

- NIST Special Publication 800-39
  Integrated Enterprise-wide Risk Management
  Organization, Mission, and Information Systems View

  Projected: January 2010

  - Incorporating public comments from NIST Special Publication 800-39, Second Public Draft
  - Incorporating three-tiered risk management approach: organization, mission/business process, and information system views
  - Incorporating cyber preparedness information
  - Providing ISO/IEC 27001 mapping to risk management publications

Key Risk Management Publication

- NIST Special Publication 800-53A, Revision 1
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations
  Projected: January 2010
  - Updating all assessment procedures to ensure consistency with NIST Special Publication 800-53, Revision 3
  - Developing new assessment procedures for information security program management controls
  - Updating web-based assessment cases for inventory of assessment procedures

Key Risk Management Publication

- NIST Special Publication 800-30, Revision 1 (Initial Public Draft)
  Guide for Conducting Risk Assessments

  Projected: January 2010

  - Down scoping current publication from risk management focus to risk assessment focus
  - Providing guidance for conducting risk assessments at each step in the Risk Management Framework
  - Incorporating threat information for cyber preparedness

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

Kelley Dempsey
(301) 975-2827
kelley.dempsey@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