Integrated Enterprise-wide Risk Management

Organization, Mission, and Information Systems View

Information System Security Association

June 16, 2009

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The Threat Situation

Continuing serious cyber attacks on federal information systems, large and small; targeting key federal 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.

Asymmetry of Cyber Warfare

The weapons of choice are—

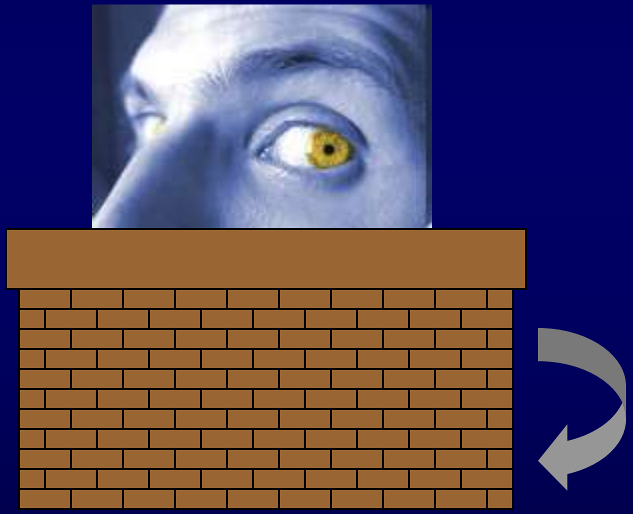
- Laptop computers, hand-held devices, cell phones.
- Sophisticated attack tools and techniques downloadable from the Internet.
- World-wide telecommunication networks including telephone networks, radio, and microwave.

Resulting in low-cost, highly destructive attack potential.

Unconventional Wisdom

NEW RULE: *Boundary protection is no longer sufficient against high-end threats capable of launching sophisticated cyber attacks...*

- Complexity of IT products and information systems.
- Insufficient penetration resistance (trustworthiness) in commercial IT products.
- Insufficient application of information system and security engineering practices.
- Undisciplined behavior and use of information technology and systems by individuals.



The Fundamentals

Fighting and winning a 21st century cyber war requires 21st century strategies, tactics, training, and technologies…

- Integration of information security into enterprise architectures and system life cycle processes.
- Common, shared information security standards for unified cyber command.
- Enterprise-wide, risk-based protection strategies.
- Flexible and agile selection / deployment of safeguards and countermeasures (maximum tactical advantage based on missions / environments of operation).
- More resilient, penetration-resistant information systems.
- Competent, capable cyber warriors.

Compliance vs. Risk-based Protection

"We should not be consumed with counting the number of dead bolts on the front door when the back door is wide open..."

-- Anonymous

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.

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.

- Employ systems and security engineering techniques to develop more secure (penetration-resistant) information systems.

Tactical Initiatives

The Short-term View

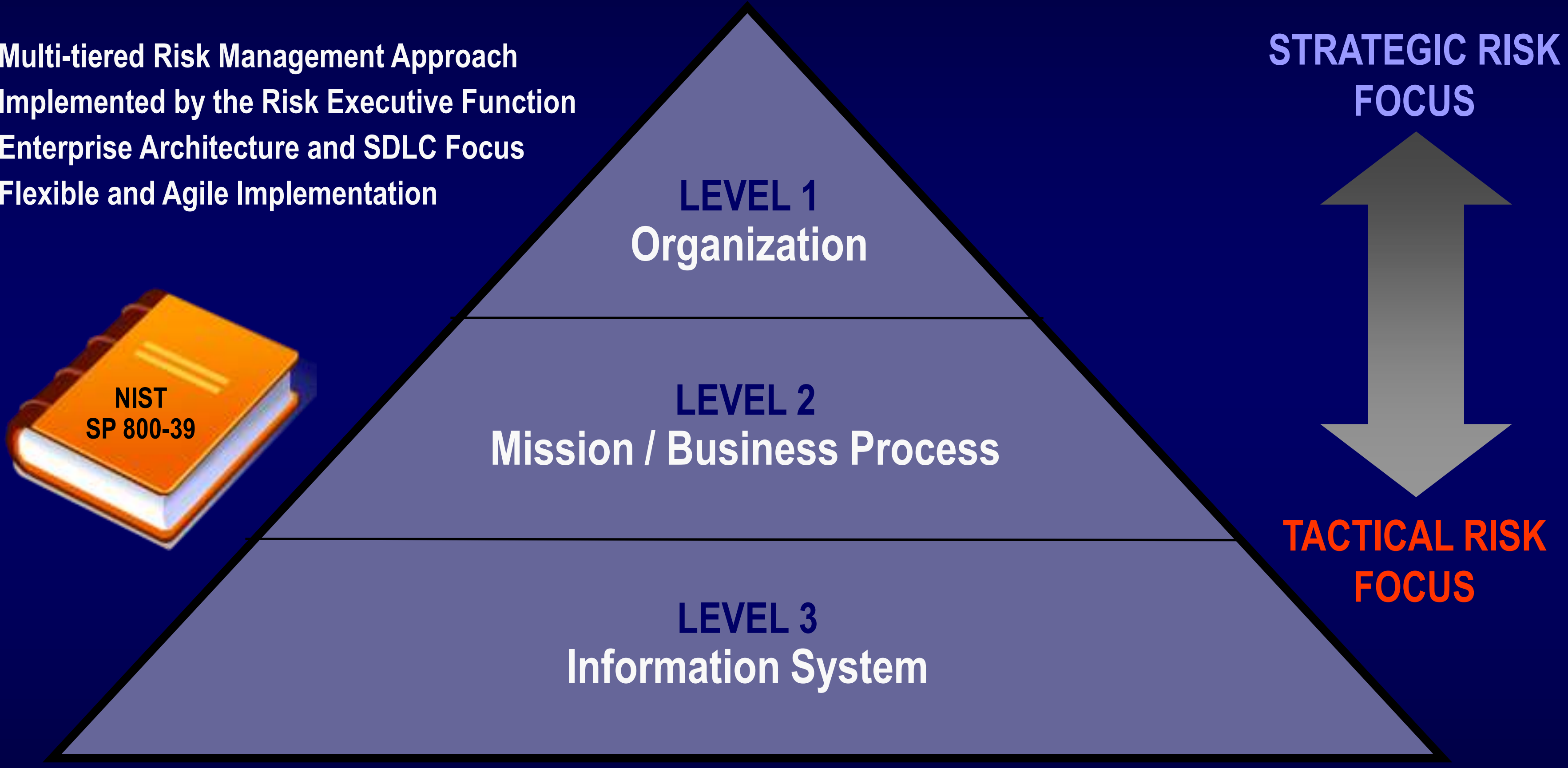
- Update security controls catalog and baselines.
  - **Delivery vehicle: NIST Special Publication 800-53, Revision 3**
- Develop enterprise-wide risk management guidance.
  - **Delivery vehicle: NIST Special Publication 800-39**
- Restructure the current certification and accreditation process for information systems.
  - **Delivery vehicle: NIST Special Publication 800-37, Revision 1**
- Provide more targeted guidance on risk assessments.
  - **Delivery vehicle: NIST Special Publication 800-30, Revision 1**

Change the Culture

- Strong, top-level senior leadership commitment.
    - **Understand adversary capabilities, types of threats and attacks.**
    - **Recognize information security is essential for mission success.**
- Employ more discipline and structure in how information systems are implemented and used.
    - **Implement least privilege, least functionality.**
    - **Require corporate and individual responsibility and accountability.**
- Develop a cyber warrior mentality.
    - **Obtain situational awareness during day-to-day agency operations.**
    - **Require ongoing monitoring of people, processes, and technologies.**

Risk Management Hierarchy

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



NIST
SP 800-39

LEVEL 1
Organization

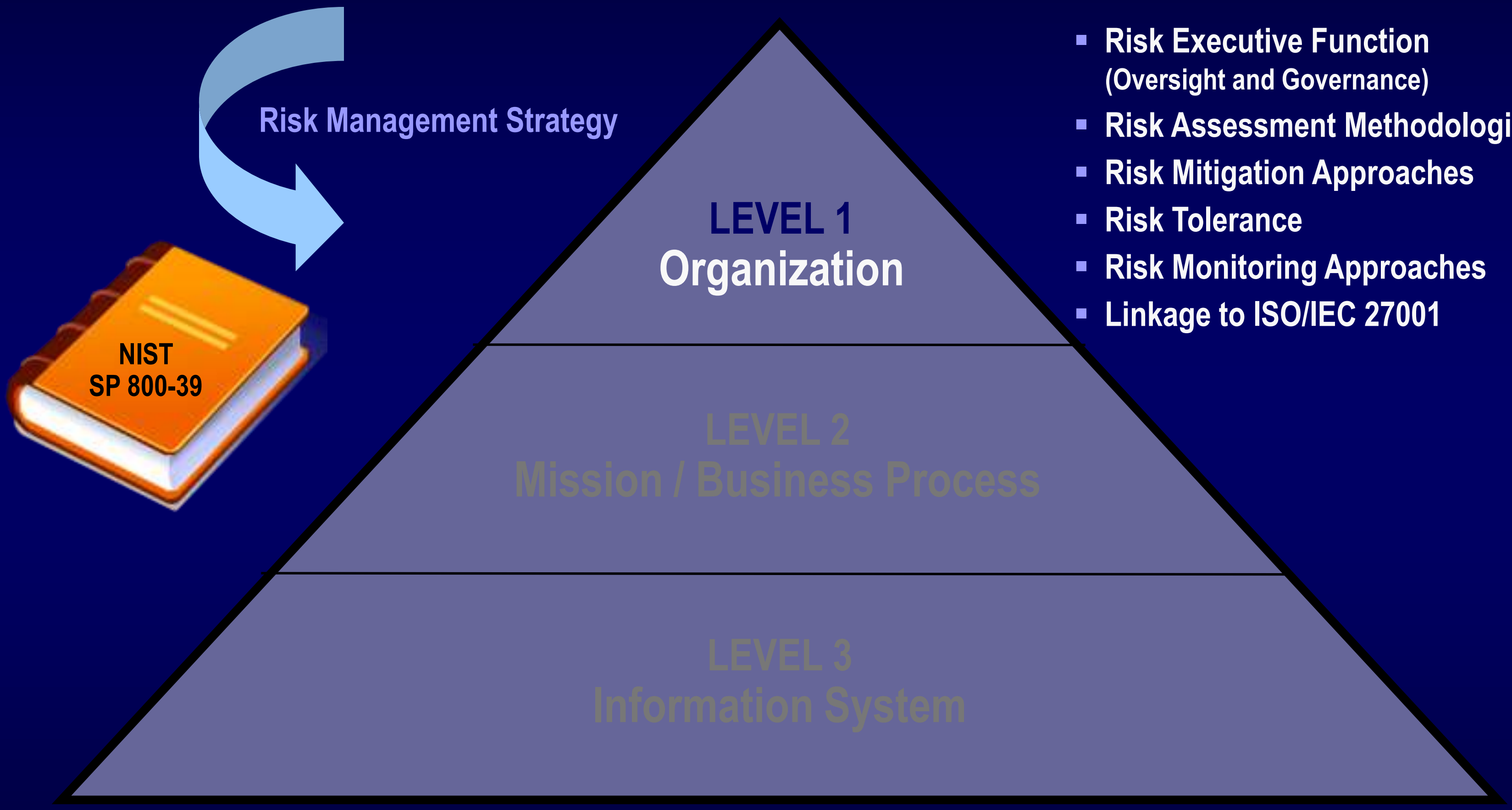
LEVEL 2
Mission / Business Process

LEVEL 3
Information System

STRATEGIC RISK
FOCUS

TACTICAL RISK
FOCUS

Risk Management Hierarchy



Risk Management Strategy

NIST
SP 800-39

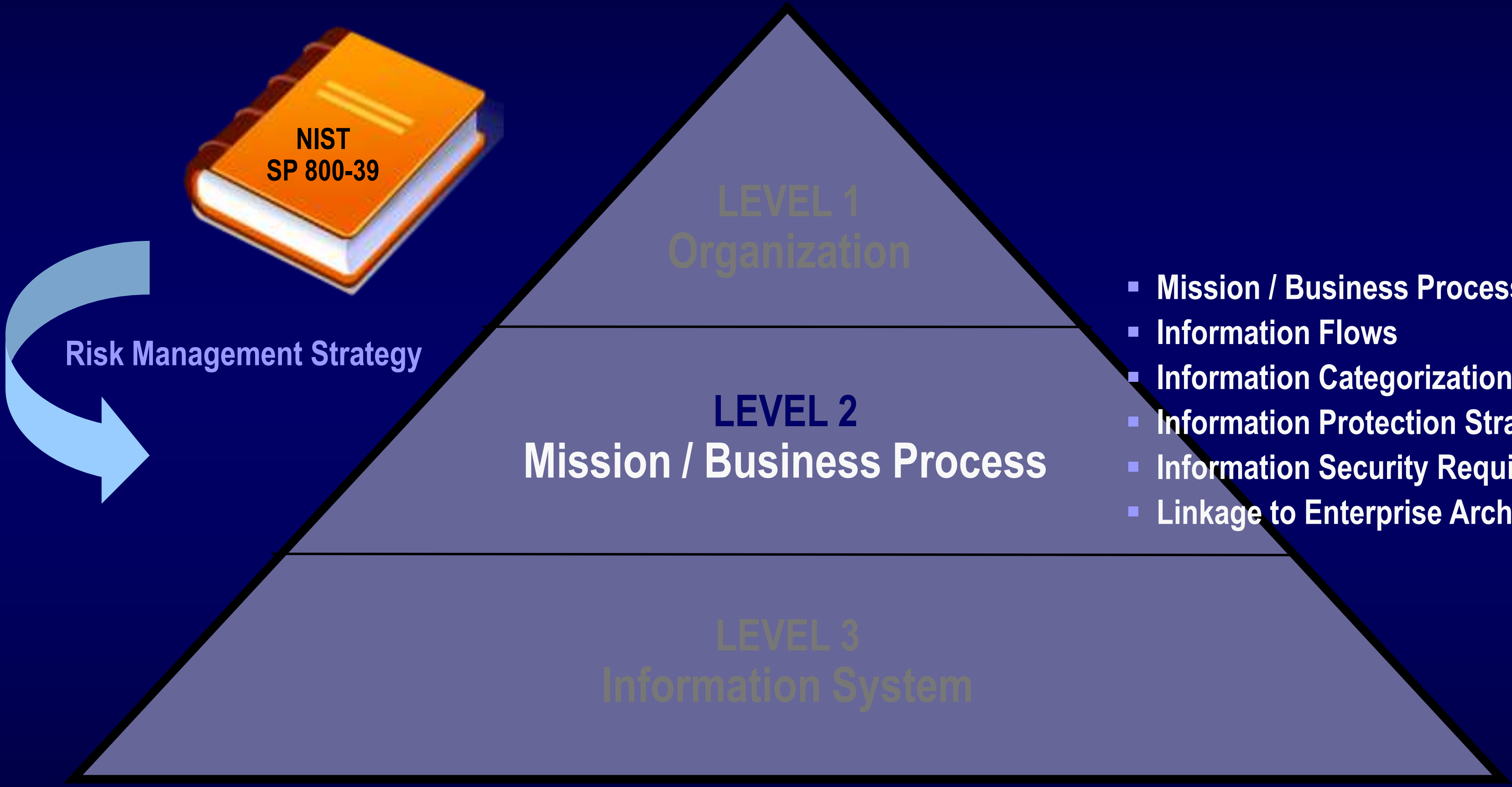
LEVEL 1
Organization

LEVEL 2
Mission / Business Process

LEVEL 3
Information System

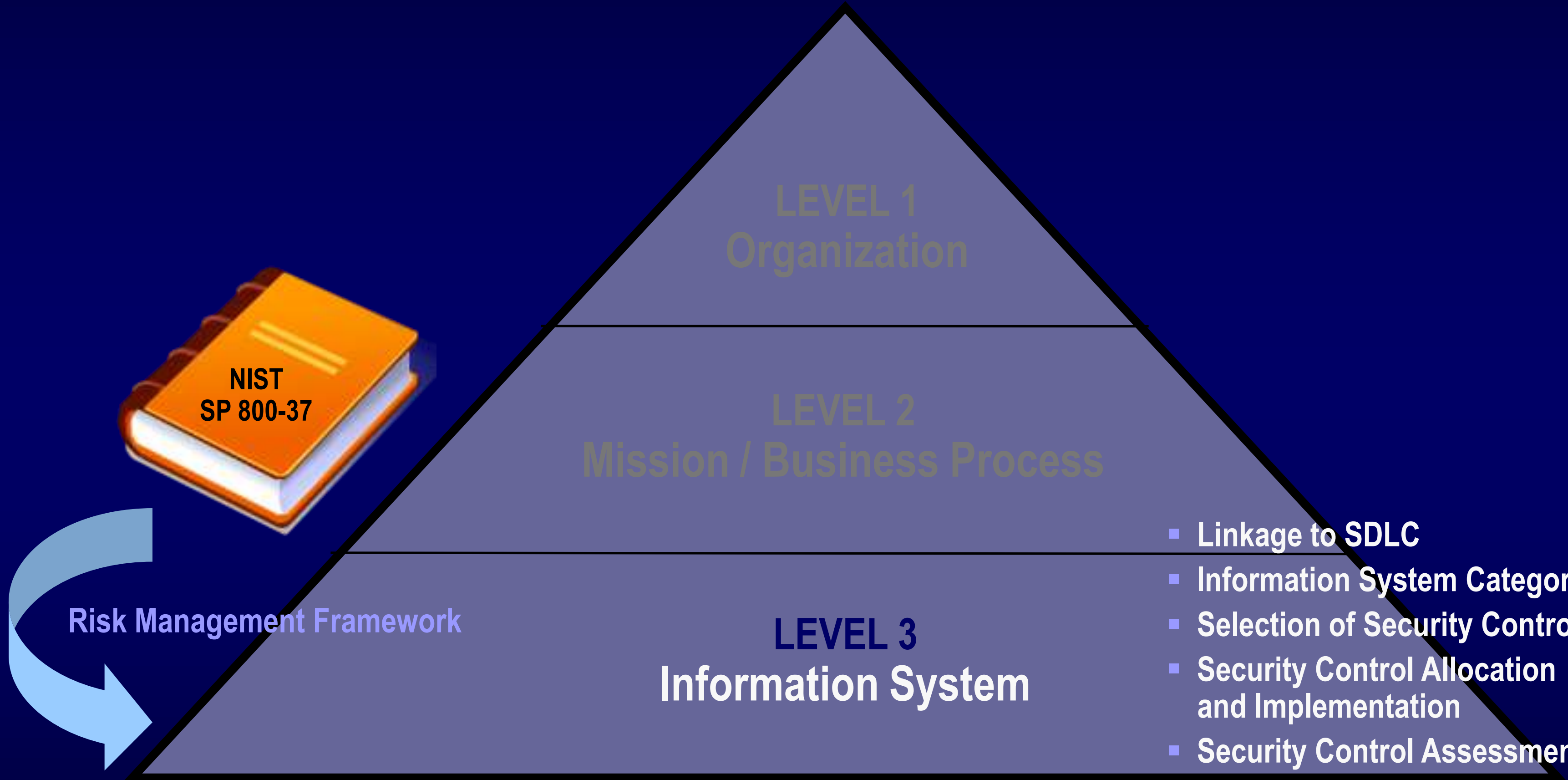
- Risk Executive Function
  (Oversight and Governance)
- Risk Assessment Methodologies
- Risk Mitigation Approaches
- Risk Tolerance
- Risk Monitoring Approaches
- Linkage to ISO/IEC 27001

Risk Management Hierarchy



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

Risk Management Hierarchy



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

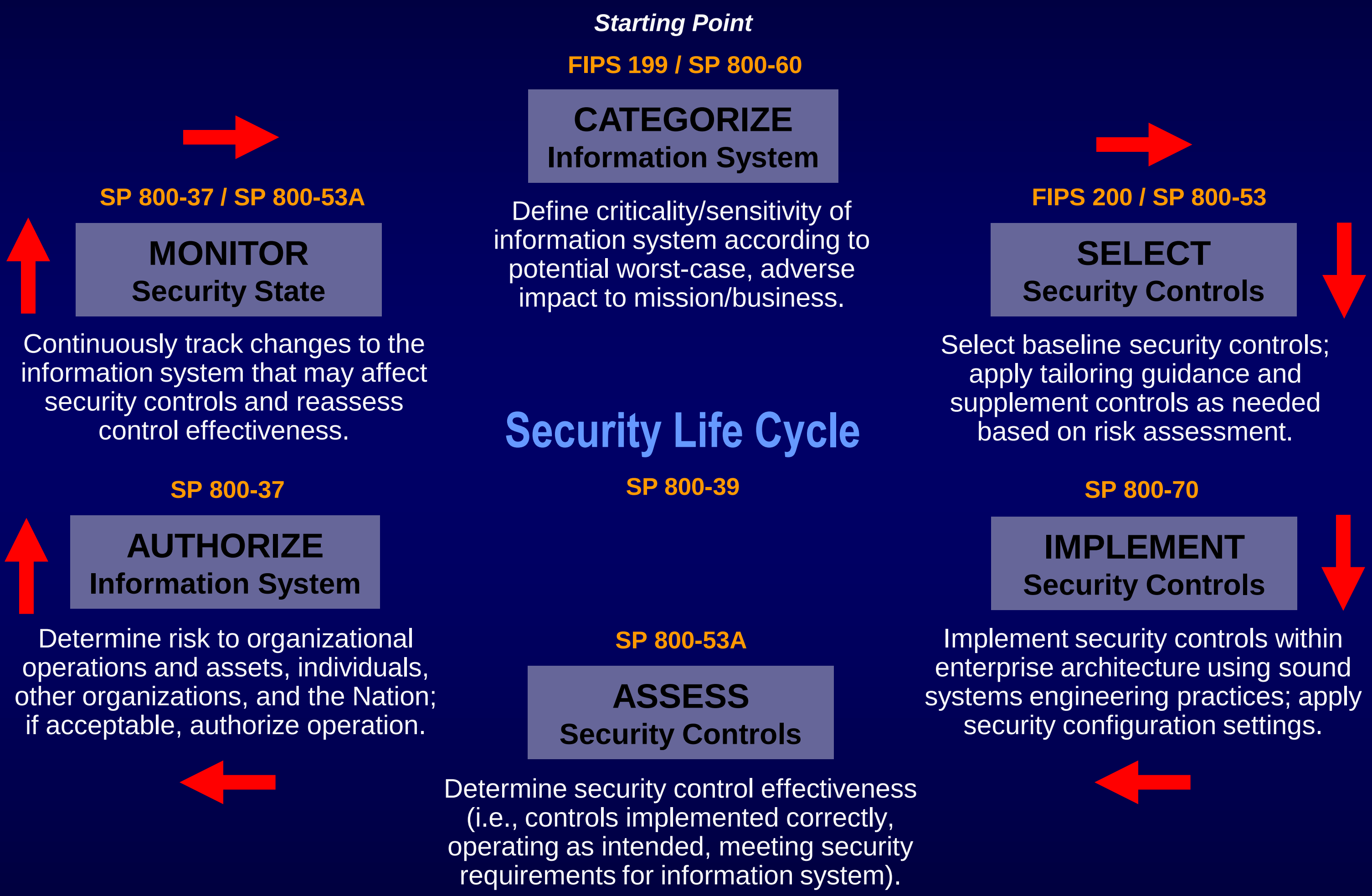
The Central Question

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)**

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

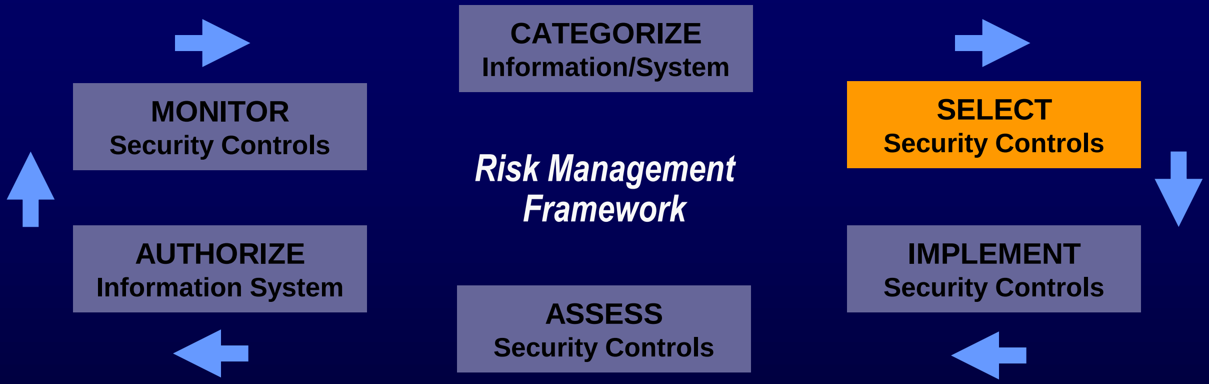
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

SP 800-39

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)



CATEGORIZE
Information/System

SELECT
Security Controls

IMPLEMENT
Security Controls

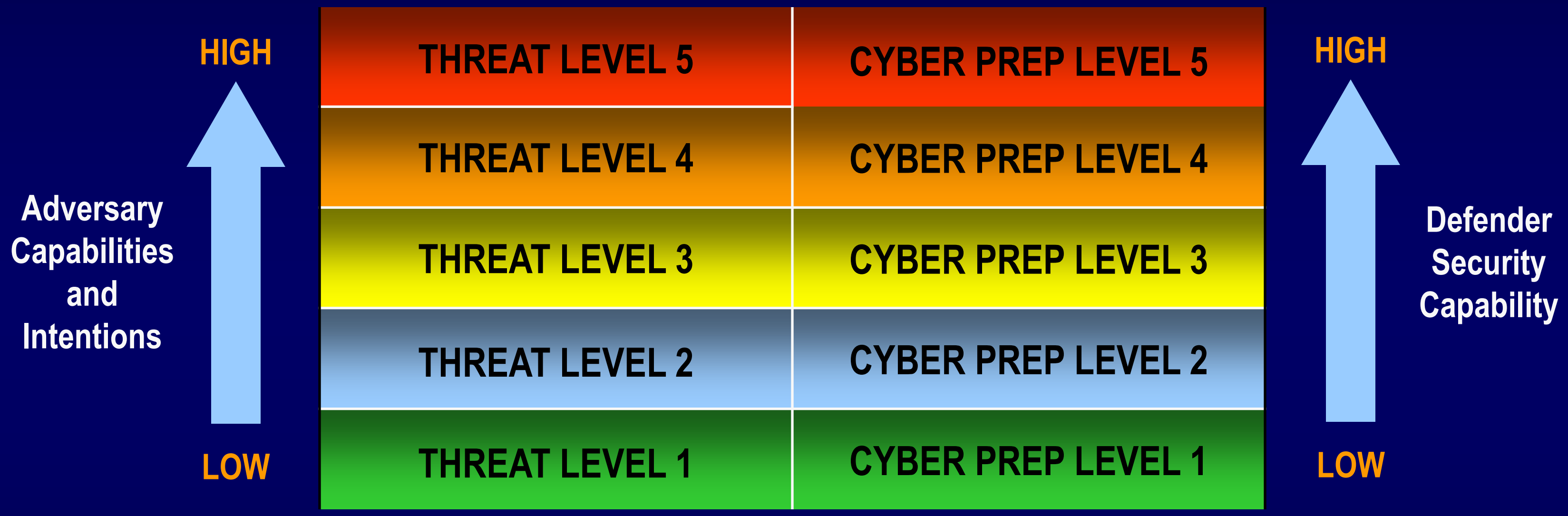
ASSESS
Security Controls

AUTHORIZE
Information System

MONITOR
Security Controls

Risk Management Framework

Cyber Preparedness



HIGH
Adversary Capabilities and Intentions
LOW
HIGH
Defender Security Capability
LOW

THREAT LEVEL 5	CYBER PREP LEVEL 5
THREAT LEVEL 4	CYBER PREP LEVEL 4
THREAT LEVEL 3	CYBER PREP LEVEL 3
THREAT LEVEL 2	CYBER PREP LEVEL 2
THREAT LEVEL 1	CYBER PREP LEVEL 1

An increasingly sophisticated and motivated threat requires increasing preparedness…

Dual Protection Strategies

- **Boundary Protection**

  Primary Consideration: ***Penetration Resistance***

  Adversary Location: ***Outside the Defensive Perimeter***

  Objective: ***Repelling the Attack***

- **Agile Defense**

  Primary Consideration: ***Information System Resilience***

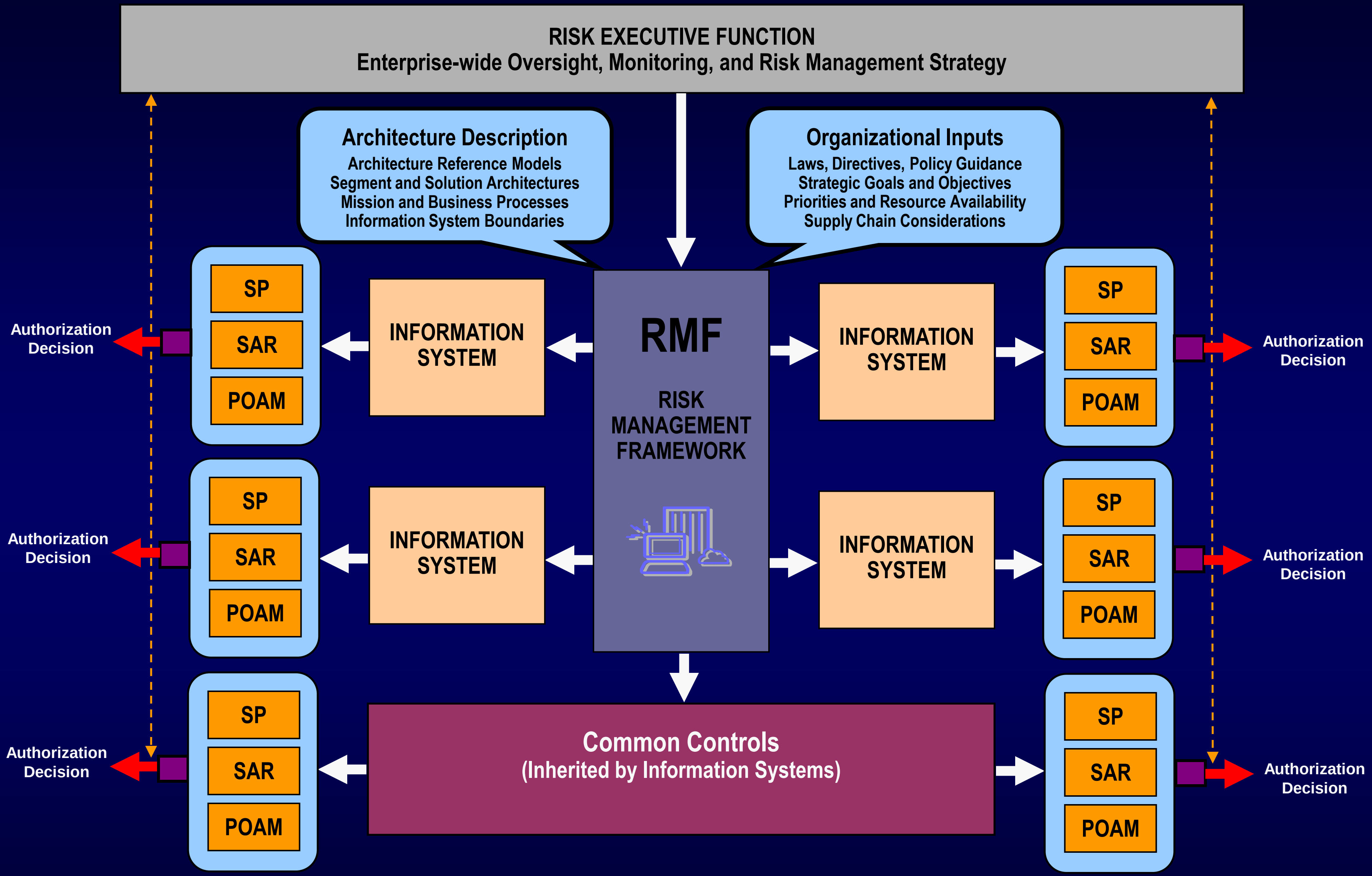
  Adversary Location: ***Inside the Defensive Perimeter***

  Objective: ***Operating while under Attack***

Agile Defense

- Boundary protection is a necessary but not sufficient condition for *Agile Defense*
- Examples of *Agile Defense* measures:
  - Compartmentalization and segregation of critical assets
  - Targeted allocation of security controls
  - Virtualization and obfuscation techniques
  - Encryption of data at rest
  - Limiting of privileges
  - Routine reconstitution to known secure state

Bottom Line: Limit damage of hostile attack while operating in a (potentially) degraded mode…



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

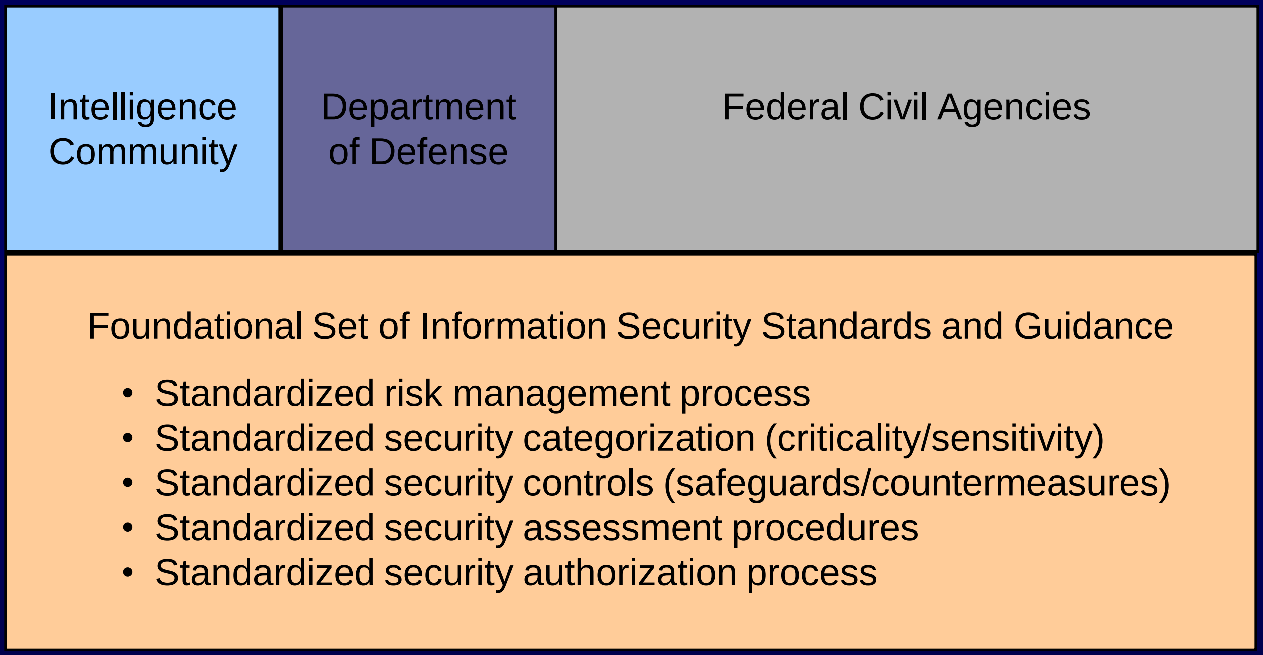
A Unified Framework

For Information Security

The Generalized Model

***Unique* Information Security Requirements**

The "Delta"



Intelligence Community

Department of Defense

Federal Civil Agencies

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

***Common* Information Security Requirements**

National security and non national security information systems

Key Risk Management Publication

- NIST Special Publication 800-53, Revision 3 (Final Public Draft)
  Recommended Security Controls for Federal Information Systems
  Projected: May 2009
  - Updating all material from NIST Special Publication 800-53, Revision 2
  - Incorporating lessons learned from interagency assessment case project
  - Incorporating material 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 (Final Public Draft)
  Applying the Risk Management Framework to Federal Information Systems
  Projected: June 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 (Third Public Draft)
  Managing Enterprise Risk: An Integrated System Life Cycle Approach
  Projected: August 2009
  - 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 800-30, Revision 1 (Initial Public Draft)
  Guide for Conducting Risk Assessments
  Projected: September 2009
  - 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

Matt Scholl
(301) 975-2941
matthew.scholl@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