NIST SP 800-53, Revision 1
CNSS Instruction 1253

Annual Computer Security Applications Conference

December 10, 2009

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Introduction

A Unified Framework

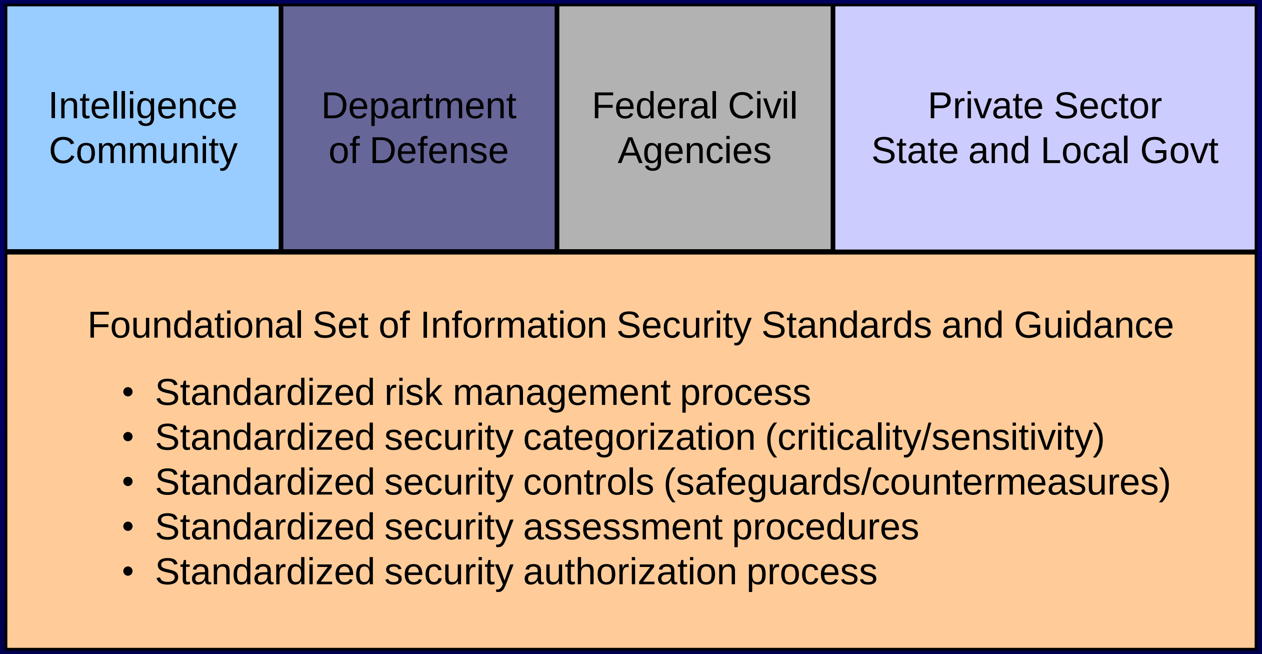
For Information Security

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

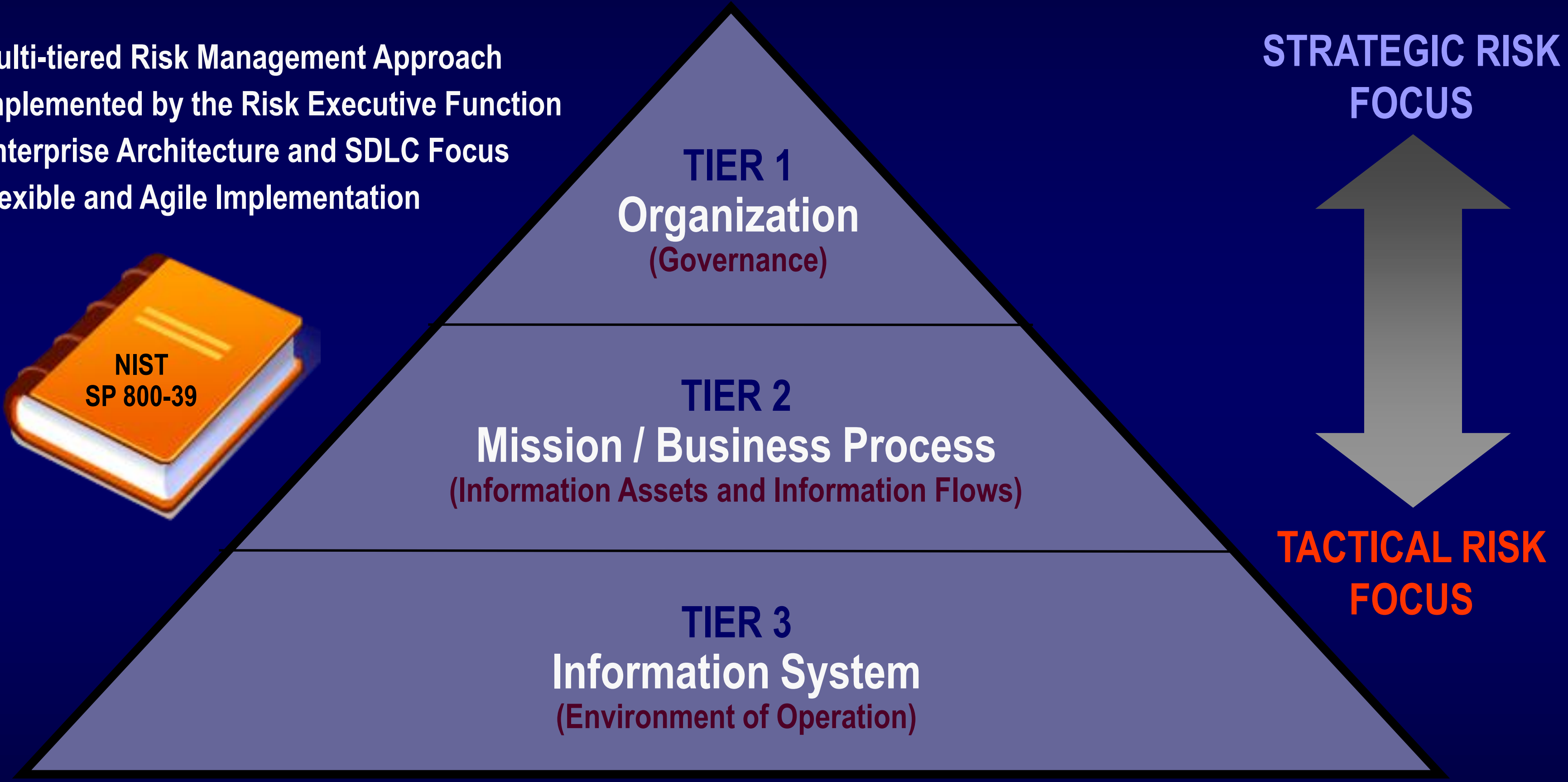
Foundational Set of Information Security Standards and Guidance

- 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

Enterprise-Wide Risk Management

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



NIST
SP 800-39

TIER 1
Organization
(Governance)

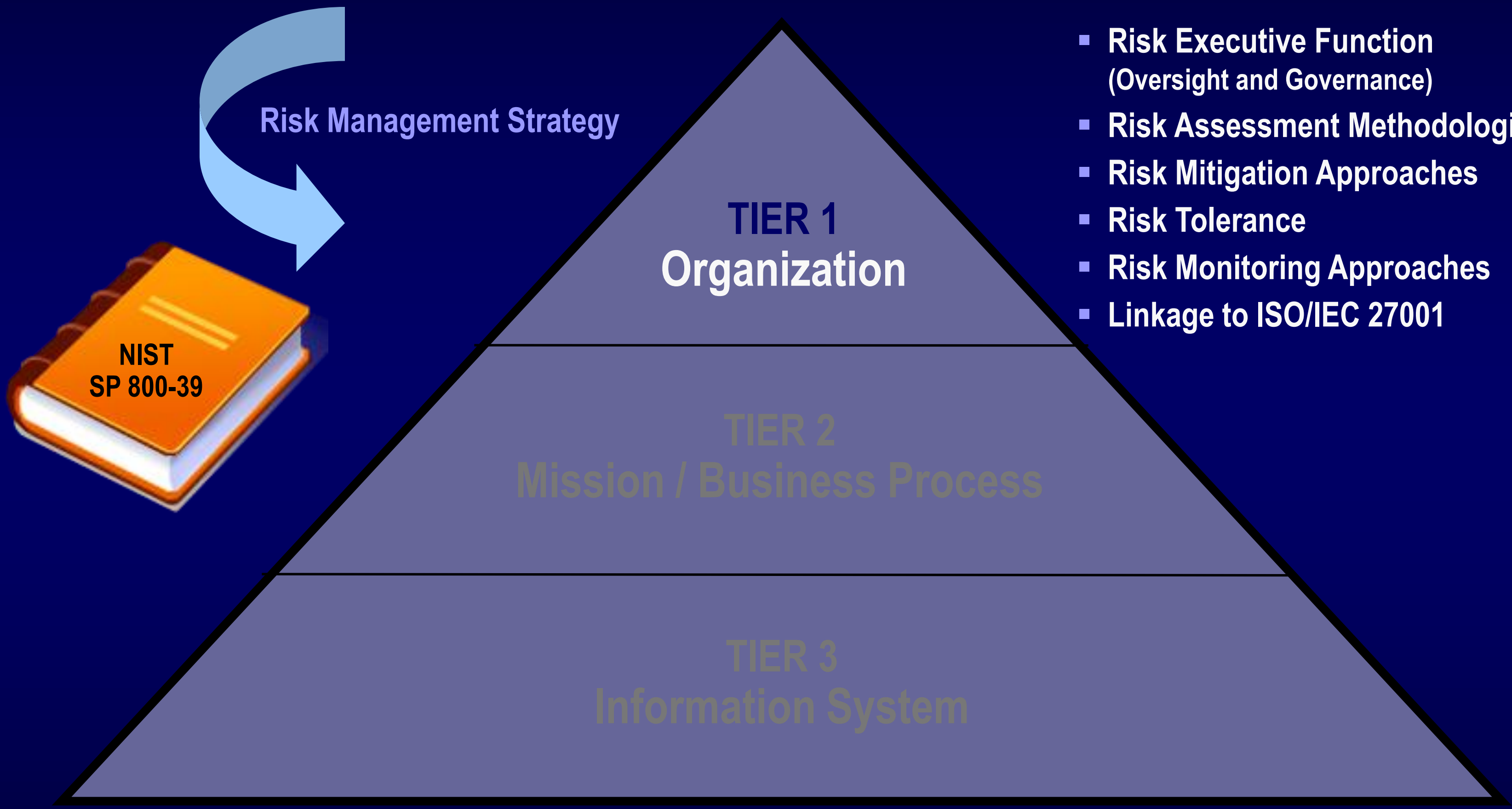
TIER 2
Mission / Business Process
(Information Assets and Information Flows)

TIER 3
Information System
(Environment of Operation)

STRATEGIC RISK FOCUS

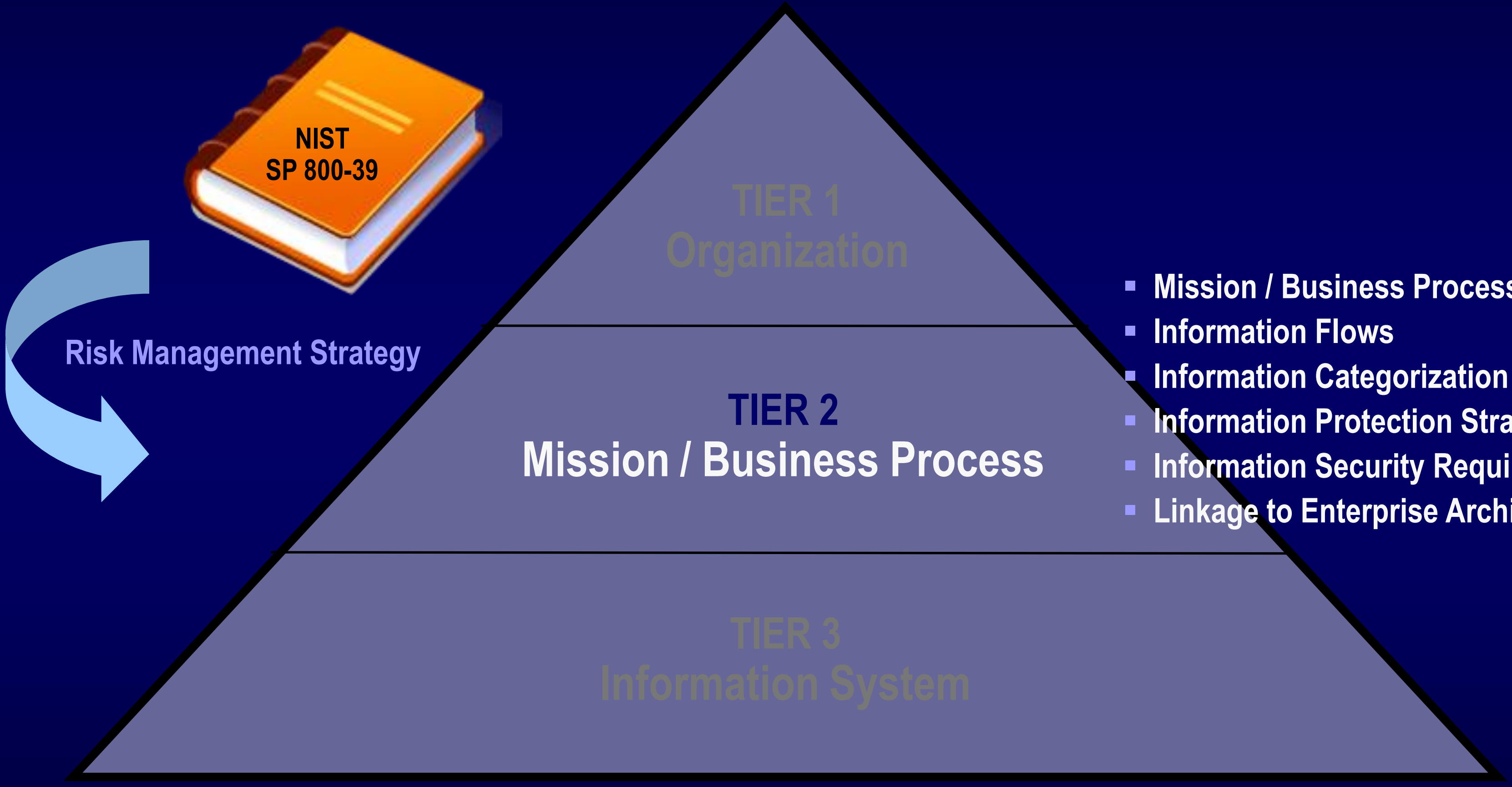
TACTICAL RISK FOCUS

Risk Management Hierarchy



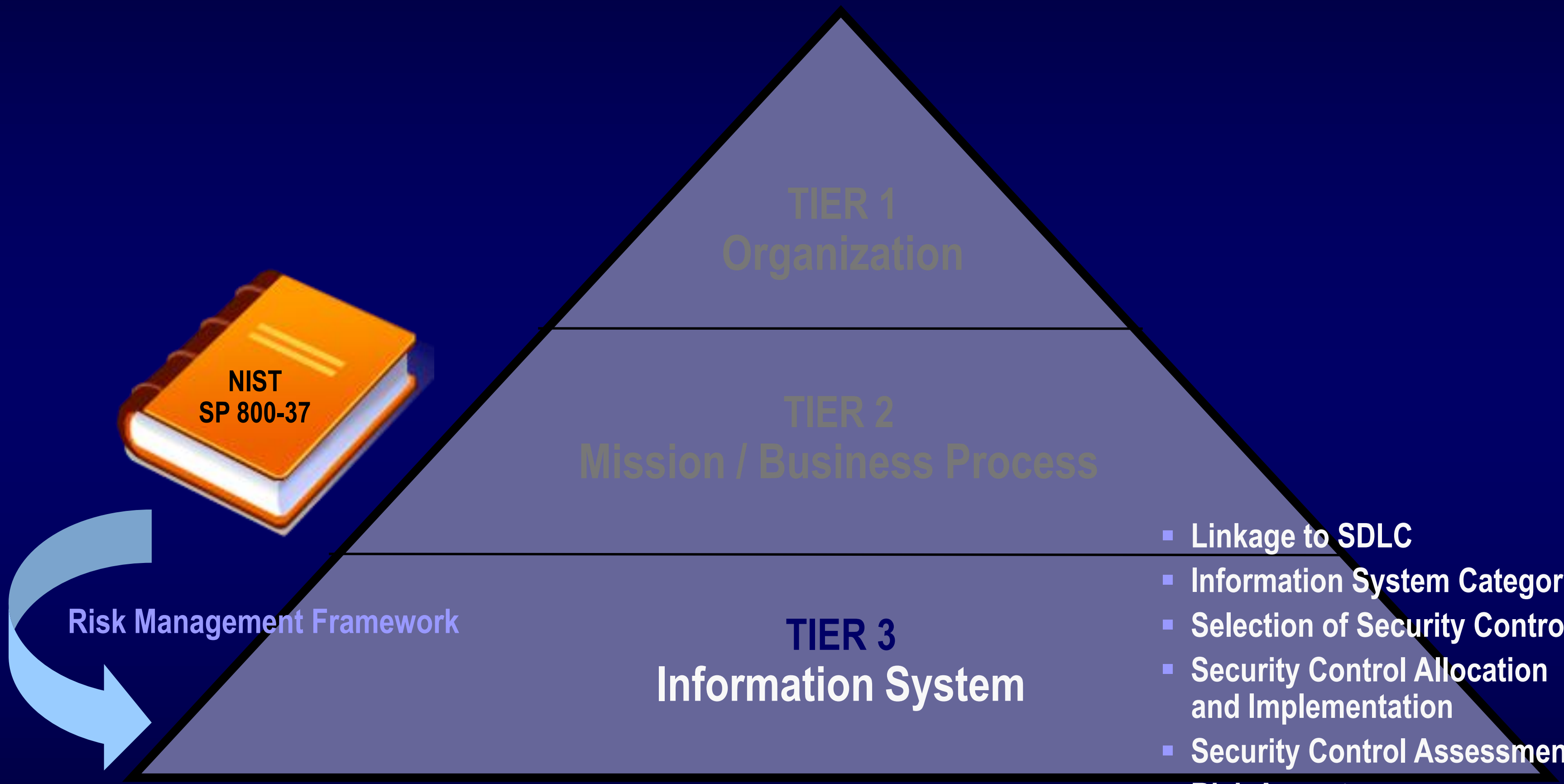
- Risk Executive Function (Oversight and Governance)
- Risk Assessment Methodologies
- Risk Mitigation Approaches
- Risk Tolerance
- Risk Monitoring Approaches
- Linkage to ISO/IEC 27001

Risk Management Hierarchy



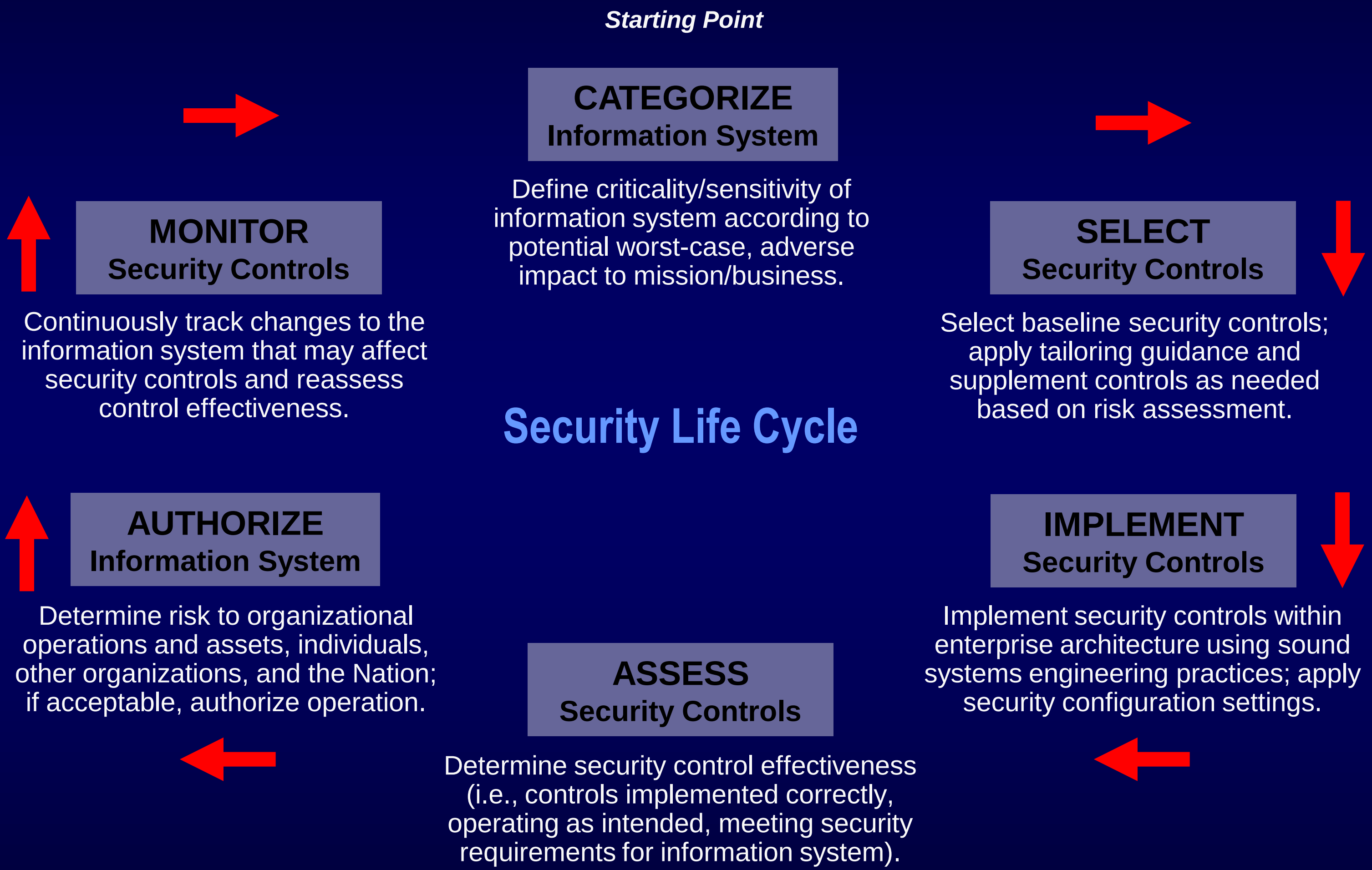
- Mission / Business Processes
- Information Flows
- Information Categorization
- Information Protection Strategy
- Information Security Requirements
- Linkage to Enterprise Architecture

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

Risk Management Framework



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 Nation; if acceptable, authorize operation.

MONITOR
Security Controls

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

Security Life Cycle

Common Security Control Catalog

- NIST Special Publication 800-53, Revision 3

  Recommended Security Controls for Federal Information Systems and Organizations

- Developed by Joint Task Force Transformation Initiative Working Group
  - *Office of the Director of National Intelligence*
  - *Department of Defense*
  - *Committee on National Security Systems*
  - *National Institute of Standards and Technology*

- Final Publication (August 2009)

Purpose
(1 of 3)

- Provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Purpose
(2 of 3)

- The guidelines have been developed to help achieve more secure information systems and effective risk management within the federal government by:
  - Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;
  - Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;

Purpose

(3of 3)

- Providing a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies;
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and
- Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

Applicability

- Federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.
- National security systems with the approval of federal officials exercising policy authority over such systems.

State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

Target Audience

- Individuals with mission/business ownership responsibilities or fiduciary responsibilities.
- Individuals with information system development and integration responsibilities.
- Individuals with information system and/or security management/oversight responsibilities.
- Individuals with information system and security control assessment and monitoring responsibilities.
- Individuals with information security implementation and operational responsibilities.

The Fundamentals

Security Controls

- The management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Classes of Security Controls

- Management Controls
  - Security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
- Operational Controls
  - Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
- Technical Controls
  - Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Security Control Families and Classes

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

SP 800-53 Defense-in-Depth

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?

Security Control Structure

(1 of 2)

- The security control structure consists of the following components:
  - Control section;
  - Supplemental guidance section;
  - Control enhancements section;
  - References section; and
  - Priority and baseline allocation section.

Security Control Structure
(2 of 2)

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

1) **The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].**
2) **The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].**
3) **The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects; delays*] network traffic above those thresholds.**
4) **The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.**

References: None.

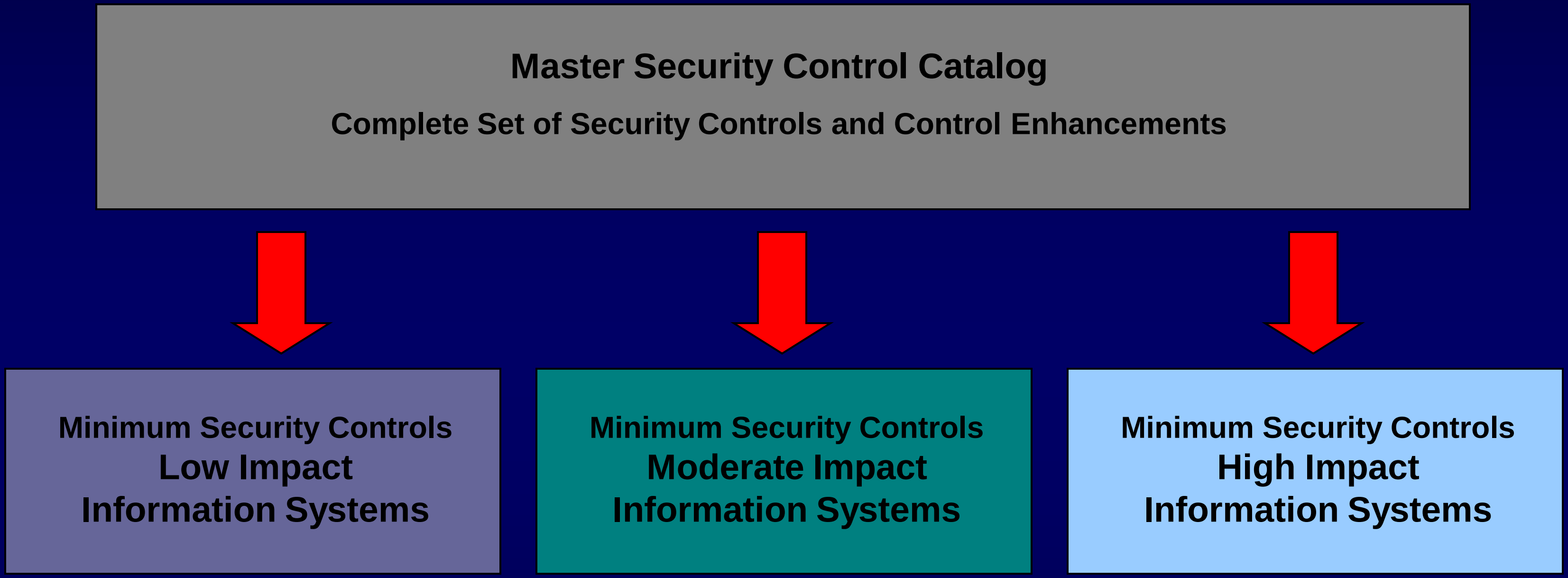
Priority and Baseline Allocation: P1 **LOW** AU-5 **MOD** AU-5 **HIGH** AU-5 (1) (2)

Security Control Baselines

- Starting point for the security control selection process.
- Chosen based on the security category and associated impact level of the information system determined in accordance with FIPS 199 and FIPS 200, respectively.
- Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact information-system levels.
- Appendix D provides a listing of baseline security controls.

Security Control Baselines

(Appendix D)



Master Security Control Catalog

Complete Set of Security Controls and Control Enhancements

Minimum Security Controls
Low Impact
Information Systems

Minimum Security Controls
Moderate Impact
Information Systems

Minimum Security Controls
High Impact
Information Systems

Baseline #1

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

Baseline #2

Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Baseline #3

Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Tailored Security Control Baselines

- Security control baselines from Appendix D adjusted in accordance with tailoring guidance.
- Minimum set of security controls for information systems.
- Supplements to the tailored baseline will likely be necessary in order to achieve adequate risk mitigation.
- Supplementation based on organizational assessment of risk with resulting controls documented in security plan.

Security Control Tailoring Process

- Applying scoping guidance to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline.
- Selecting (or specifying) compensating security controls, if needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement.
- Specifying organization-defined parameters in the security controls via explicit assignment and selection statements.

Scoping Guidance
(1 of 2)

- Common control-related considerations.
- Security objective-related considerations.
- System component allocation-related considerations.
- Technology-related considerations.
- Physical infrastructure-related considerations.
- Policy/regulatory-related considerations.

Scoping Guidance
(2 of 2)

- Operational/environmental-related considerations.
- Scalability-related considerations.
- Public access-related considerations.

Compensating Controls

(1 of 2)

- Management, operational, or technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of a recommended security controls in the low, moderate, or high baselines described in Appendix D, that provides equivalent or comparable levels of protection for an information system and the information processed, stored, or transmitted by that system.

Compensating Controls
(2 of 2)

- The organization:
  - Selects the compensating control from Special Publication 800-53, Appendix F, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source.
  - Provides supporting rationale for how the compensating control delivers an equivalent security capability for the information system and why the related baseline security control could not be employed.
  - Assesses and accepts the risk associated with employing the compensating control in the information system.

Security Control Parameterization

(1 of 2)

- Organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define certain portions of the controls to support specific organizational requirements or objectives.
- Organizations review the list of security controls for assignment and selection operations and determine the appropriate organization-defined values for the identified parameters.

Security Controls Parameterization

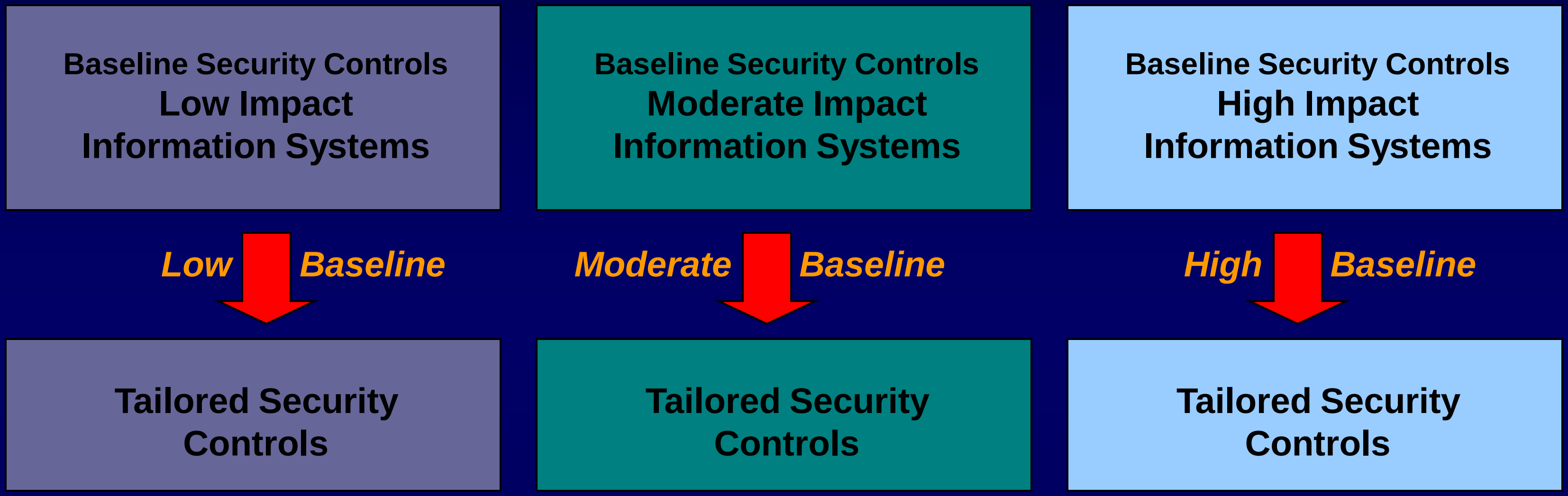
(2 of 2)

- Values for organization-defined parameters are adhered to unless more restrictive values are prescribed by applicable federal laws, Executive Orders, directives, policies, standards, guidelines, or regulations.

- Organizations may specify values for security control parameters before selecting compensating controls since the specification of those parameters completes the definition of the security control and may affect the compensating control requirements.

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Baseline Security Controls
Low Impact
Information Systems

Low *Baseline*

Tailored Security Controls

Baseline Security Controls
Moderate Impact
Information Systems

Moderate *Baseline*

Tailored Security Controls

Baseline Security Controls
High Impact
Information Systems

High *Baseline*

Tailored Security Controls

Organization #1	***Organization #2***	***Organization #3***
Operational Environment #1	***Operational Environment #2***	***Operational Environment #3***

Cost effective, risk-based approach to achieving adequate information security…

Common Controls

(1 of 2)

- Security controls that are *inheritable* by one or more organizational information systems.
- Organizations assign responsibility for common controls to appropriate organizational officials and coordinate the development, implementation, assessment, authorization, and monitoring of the controls.
- Identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of senior leaders.

Common Controls

(2 of 2)

- Generally documented in the organization-wide *information security program plan* unless implemented as part of a specific information system, in which case the controls are documented in the security plan for that system.
- Common controls are authorized by senior officials with at least the same level of authority and responsibility for managing risk as the authorization officials for information systems inheriting the controls.

The Process

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 Categorization

Example: An Organizational Information System

Guidance for Mapping Types of Information and Information Systems to FIPS 199 Security Categories

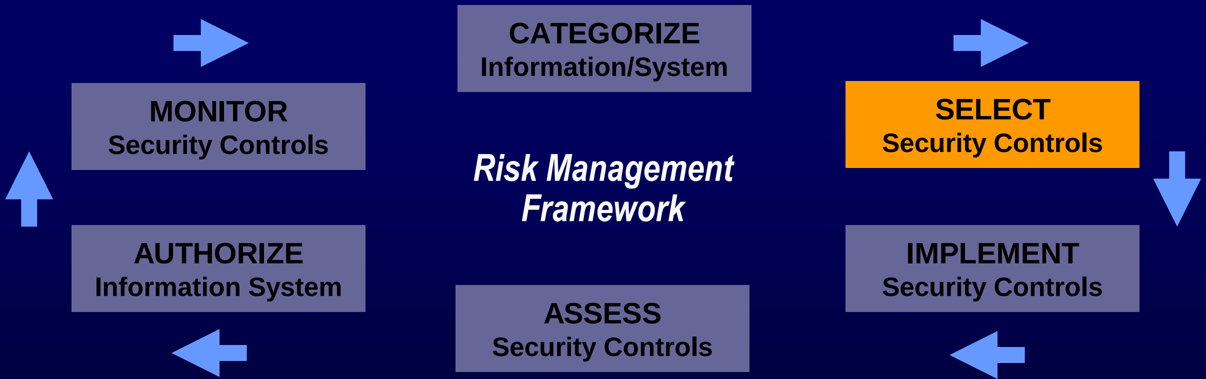
SP 800-60

FIPS 199	LOW	MODERATE	HIGH
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **se**[illegible]**atastrophic** adv[illegible]ct on org[illegible]l operations, org[illegible]l assets, or indi[illegible]
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The l[illegible]ilability could [illegible]ed to have a **sever**[illegible]**strophic** adverse e[illegible] organizatio[illegible]ons, organizational a[illegible] individuals.

Baseline Security Controls for High Impact Systems

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

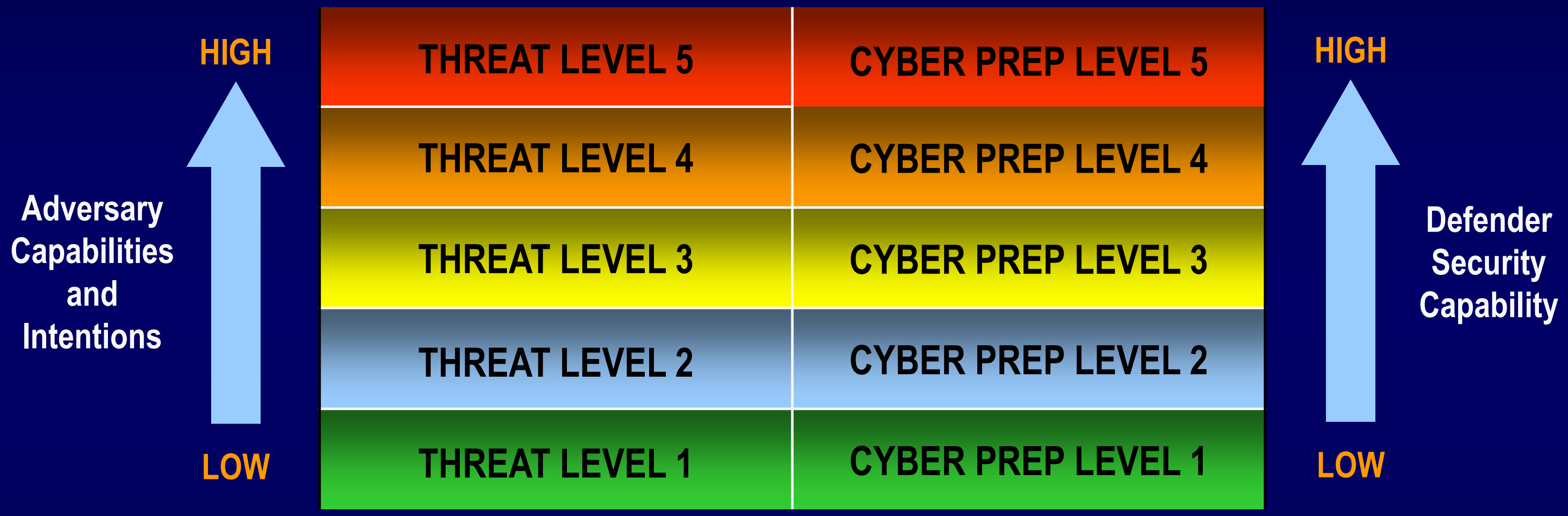
ASSESS
Security Controls

AUTHORIZE
Information System

MONITOR
Security Controls

Risk Management Framework

Cyber Preparedness



HIGH

Adversary Capabilities and Intentions

LOW

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

HIGH

Defender Security Capability

LOW

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

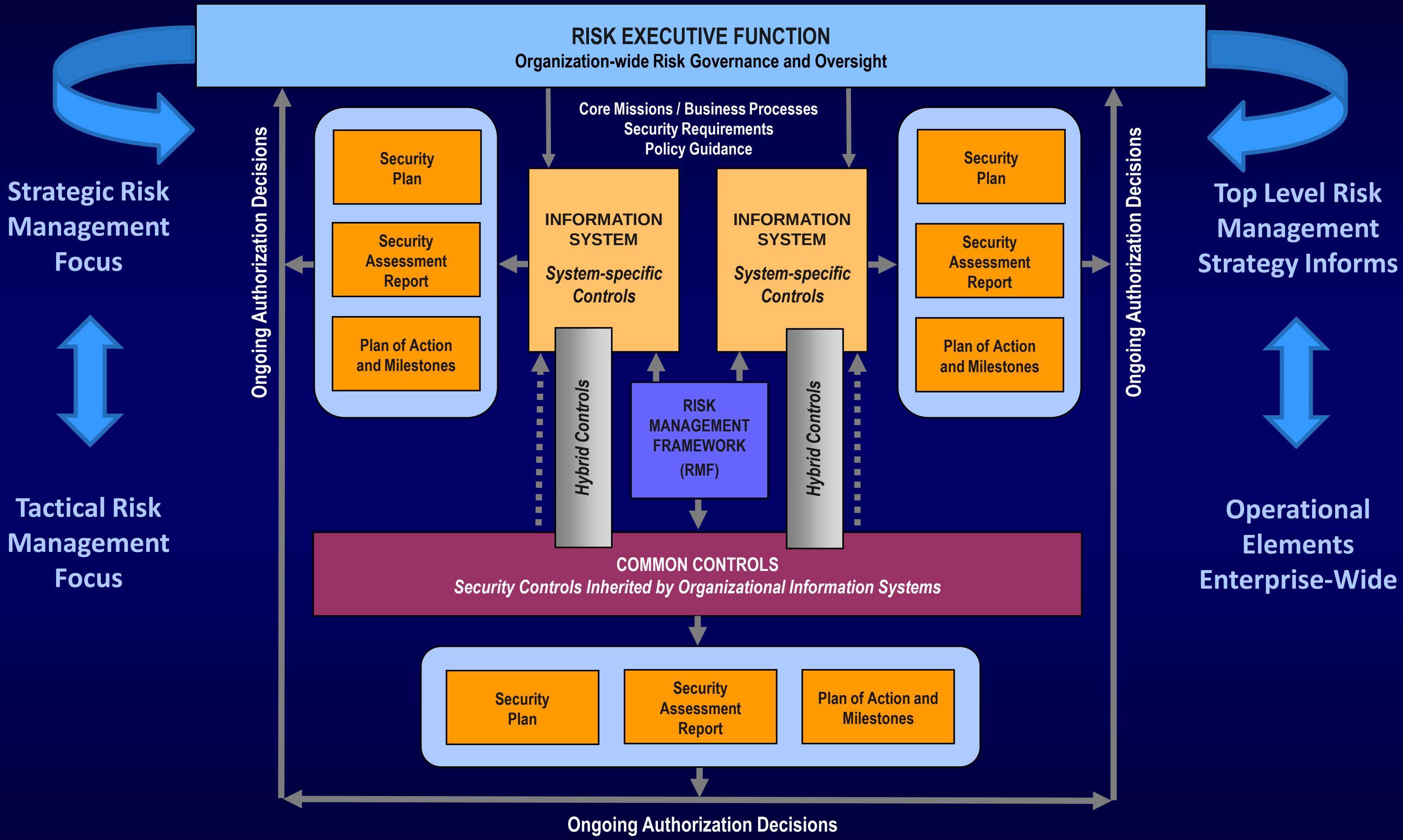
- Boundary protection is a necessary but not sufficient condition for *Agile Defense*
- Examples of *Agile Defense* measures:
  - Compartmentalization and segregation of critical assets
  - Targeted allocation of security controls
  - Virtualization and obfuscation techniques
  - Encryption of data at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

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

Security Control Allocation

- Security controls are defined to be *system-specific*, *hybrid*, or *common*.
- Security controls are *allocated* to specific components of organizational information systems as system-specific, hybrid, or common controls.
- Security control allocations are consistent with the organization’s *enterprise architecture* and *information security architecture.*

Security Control Accountability



RISK EXECUTIVE FUNCTION
Organization-wide Risk Governance and Oversight

Strategic Risk Management Focus

Tactical Risk Management Focus

Top Level Risk Management Strategy Informs

Operational Elements Enterprise-Wide

Core Missions / Business Processes
Security Requirements
Policy Guidance

Ongoing Authorization Decisions
Security Plan
Security Assessment Report
Plan of Action and Milestones
INFORMATION SYSTEM
System-specific Controls
INFORMATION SYSTEM
System-specific Controls
Security Plan
Security Assessment Report
Plan of Action and Milestones
Ongoing Authorization Decisions
Hybrid Controls
RISK MANAGEMENT FRAMEWORK (RMF)
Hybrid Controls
COMMON CONTROLS
Security Controls Inherited by Organizational Information Systems
Security Plan
Security Assessment Report
Plan of Action and Milestones
Ongoing Authorization Decisions

Major Changes in SP 800-53, Rev 3

- Provides a unified catalogue security controls for both national security and non-national security systems.
- Adds new security controls for advanced cyber threats.
- Introduces an 18th family of security controls for enterprise information security programs.
- Establishes priority codes for security controls to assist in sequencing decisions for implementation.
- Includes revised security control baseline allocations.

National Security Systems

- Follow CNSS Instruction 1253:
  - To categorize the system.
  - To select the baseline set of security controls.
    - Baseline (impact) method.
    - Control profiles method.
  - To determine variable instantiations for assignments.
- Follow NIST SP 800-53
  - For descriptions of all security controls (controls catalog).
  - For initial guidance on the security control selection process (i.e., tailoring, supplementing).

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

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov