Next Generation Risk Management

Information Security Transformation for the Federal Government

OCR/NIST
Safeguarding Health Information Conference

May 11, 2010

Patricia Toth

Computer Security Division
Information Technology Laboratory

Risk and Security

- What is the difference between risk and security?
  - Information Security

    The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

  - Risk

    A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- Types of Threats

  Purposeful attacks, environmental disruptions, and human errors.

The Cyber Threat Situation

Continuing serious cyber attacks on public and private sector information systems, large and small; targeting key 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.

What is at Risk?

- Federal information systems supporting Defense, Civil, and Intelligence agencies within the federal government.
- Information systems supporting critical infrastructures within the United States (public and private sector).
- Private sector information systems supporting U.S. industry and businesses (intellectual capital).

Producing both national security and economic security concerns for the Nation…

Need Broad-Based Security Solutions

- Over 90% of critical infrastructure systems/applications owned and operated by non federal entities.
- Key sectors:
  - 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

The Fundamentals

Combating 21st century cyber attacks requires 21st century strategies, tactics, training, and technologies…

- Integration of information security into enterprise architectures and system life cycle processes.
- Unified information security framework and common, shared security standards and guidance.
- Enterprise-wide, risk-based protection strategies.
- Flexible and agile selection and deployment of security controls (i.e., safeguards and countermeasures).
- More resilient, penetration-resistant information systems.
- Competent, capable cyber warriors.

Joint Task Force Transformation Initiative

A Broad-Based Partnership —

- National Institute of Standards and Technology
- Department of Defense
- Intelligence Community
- Committee on National Security Systems

Characteristics of Risk-Based Approaches
(1 of 3)

- Integrates information security more closely into the enterprise architecture and system development life cycle.
- Provides equal emphasis on the security control selection, implementation, assessment, and monitoring, and the authorization of information systems.
- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.

Characteristics of Risk-Based Approaches
(2 of 3)

- Links risk management activities at the organization, mission, and information system levels through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems.

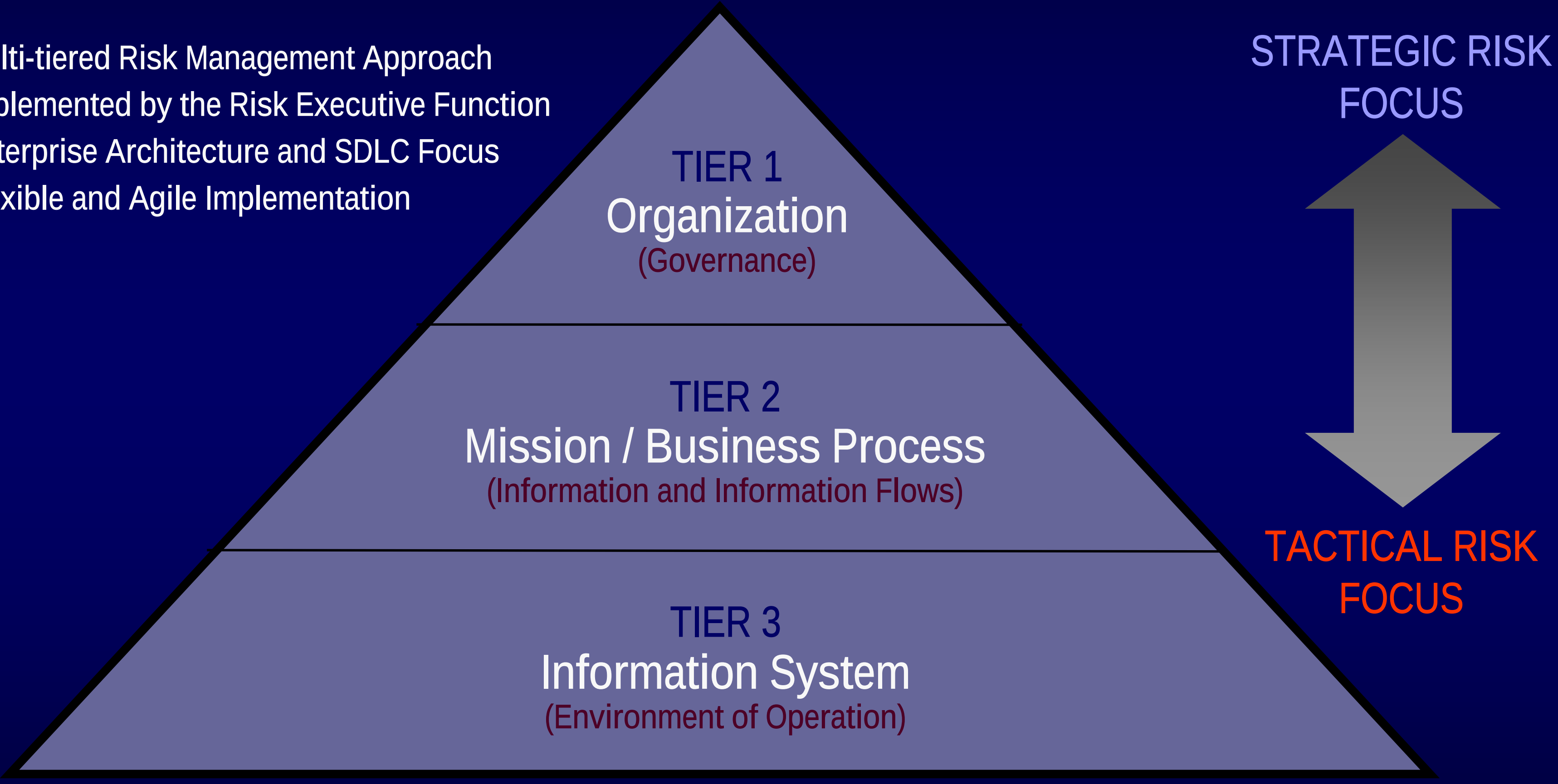
Characteristics of RMF-Based Process

(3 of 3)

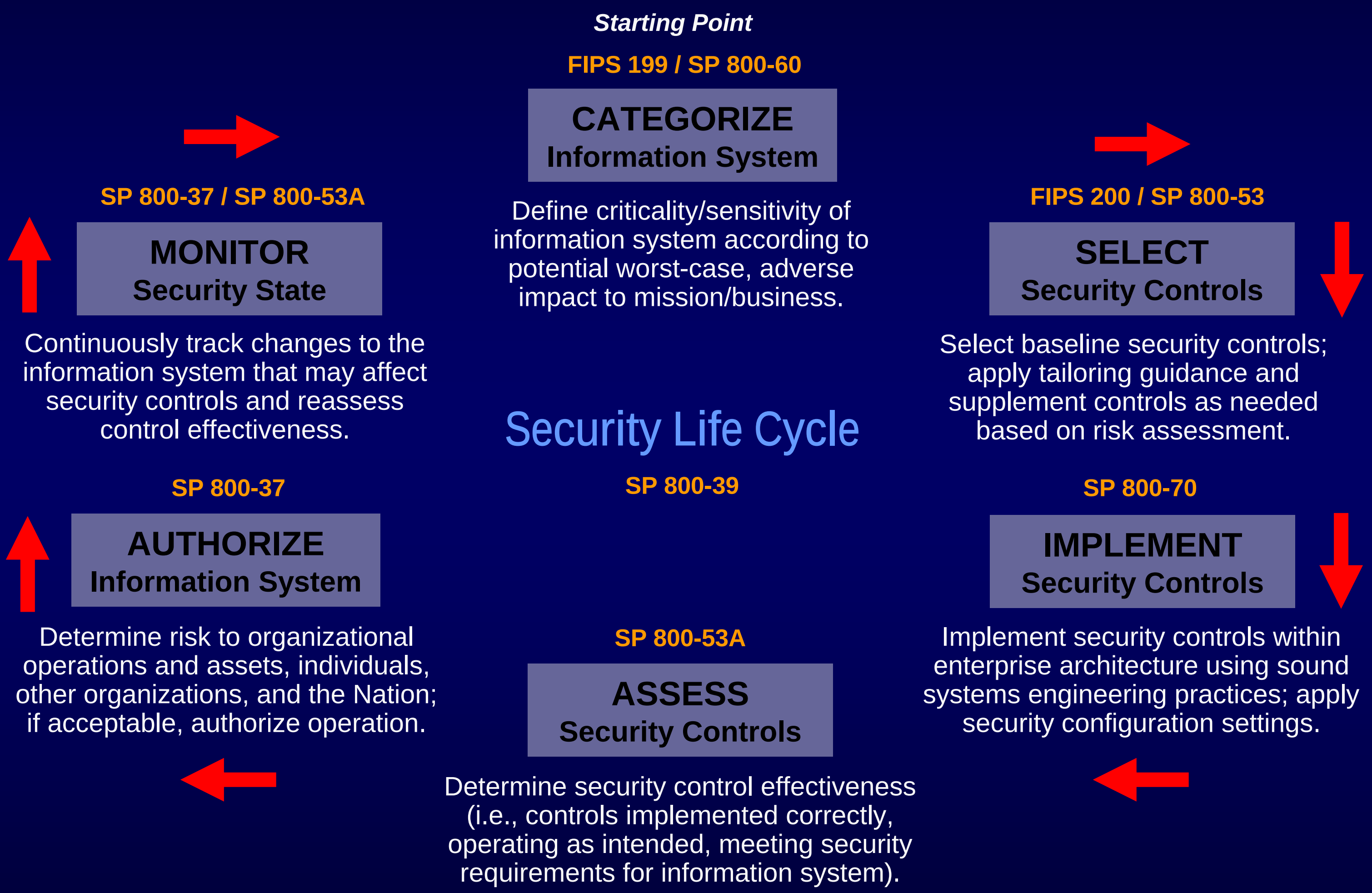
- Encourages the use of automation to:
  - Increase consistency, effectiveness, and timeliness of security control implementation and functionality; and
  - Provide senior leaders the necessary information to take credible, risk-based decisions with regard to the information systems supporting their core missions and business functions.

Enterprise-Wide Risk Management

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



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

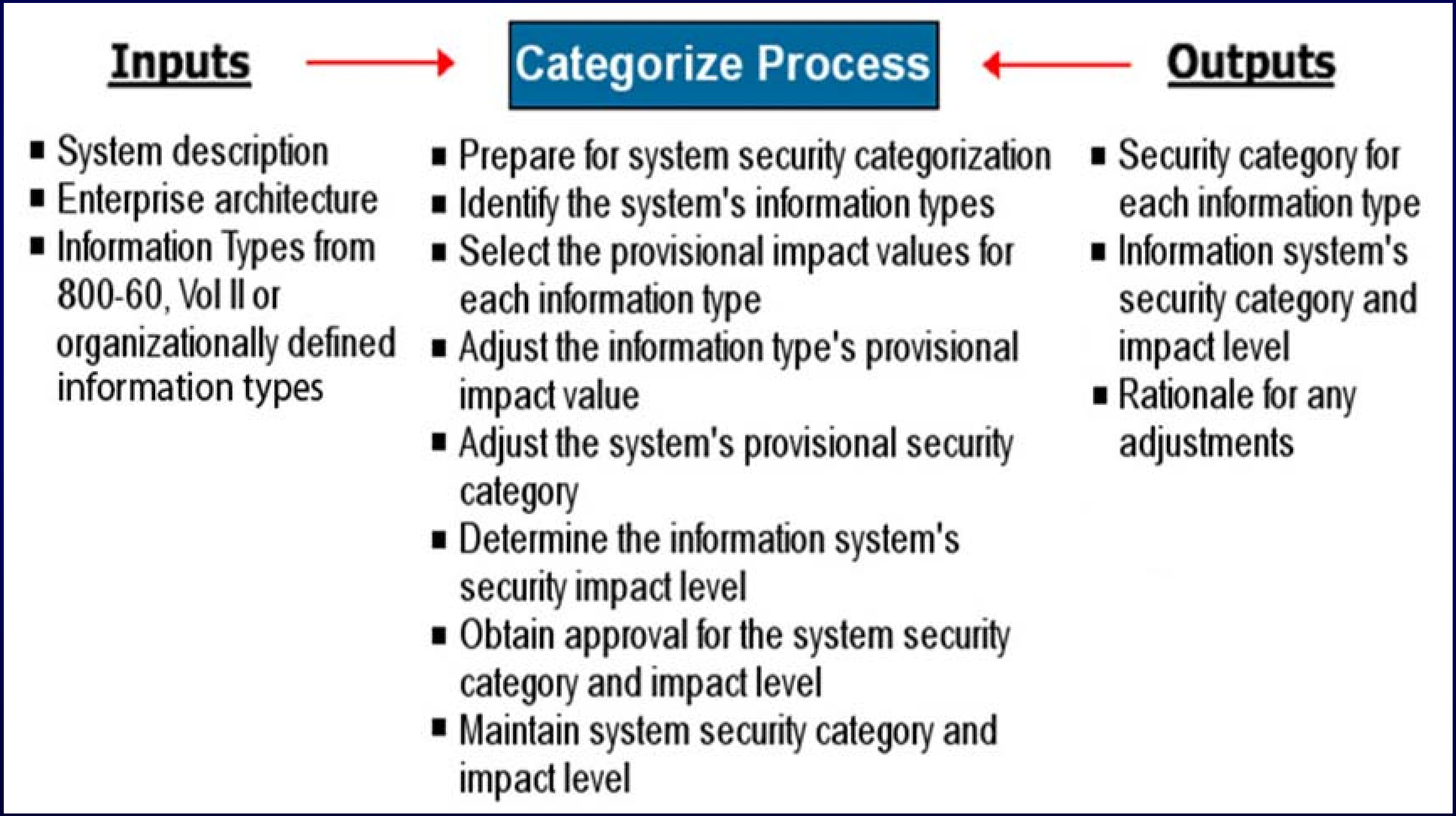
MONITOR
Security State

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

Security Life Cycle

SP 800-39

Categorize Process



Inputs

- System description
- Enterprise architecture
- Information Types from 800-60, Vol II or organizationally defined information types

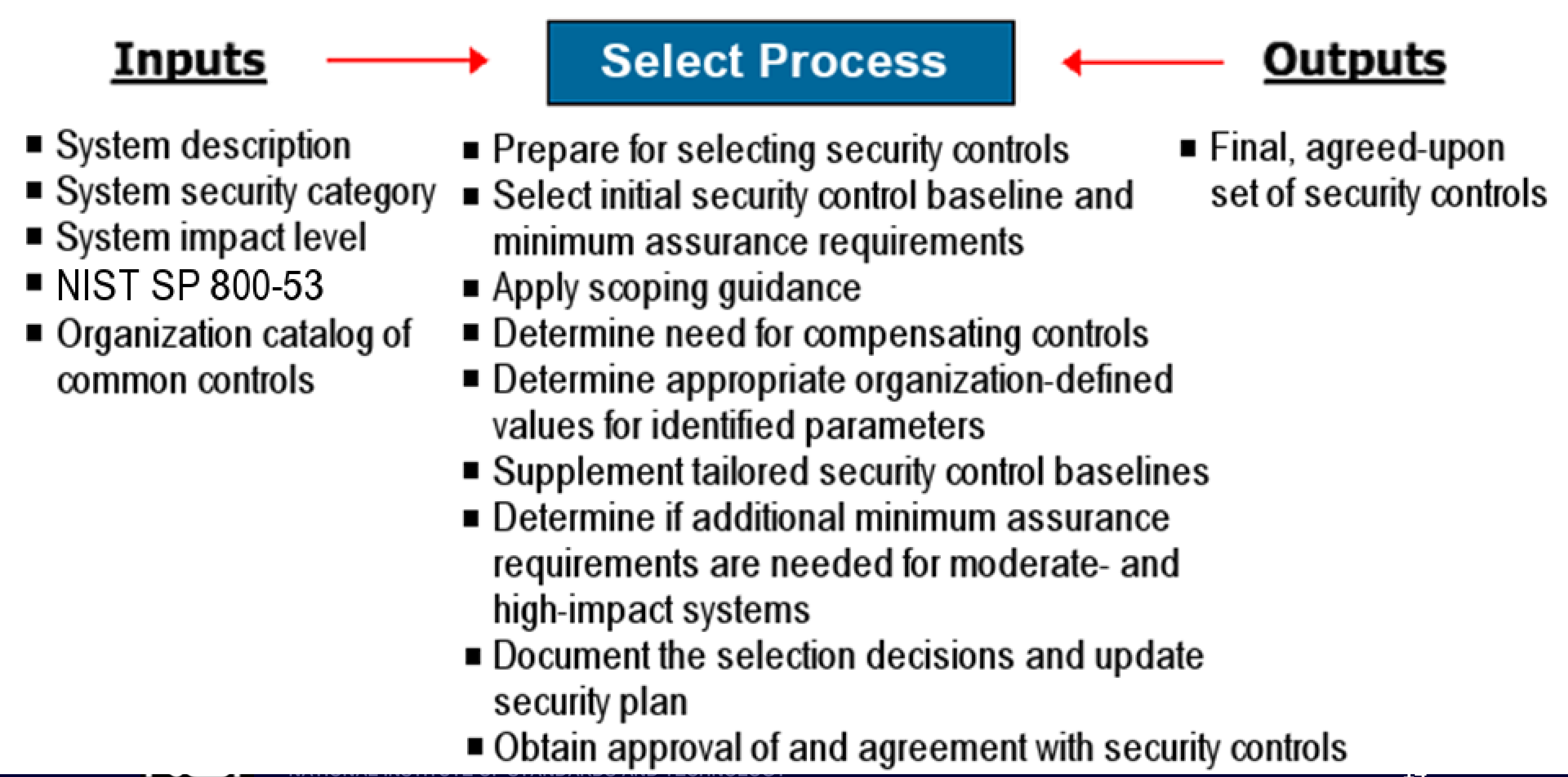
Categorize Process

- Prepare for system security categorization
- Identify the system's information types
- Select the provisional impact values for each information type
- Adjust the information type's provisional impact value
- Adjust the system's provisional security category
- Determine the information system's security impact level
- Obtain approval for the system security category and impact level
- Maintain system security category and impact level

Outputs

- Security category for each information type
- Information system's security category and impact level
- Rationale for any adjustments

Select Process



Inputs → **Select Process** ← **Outputs**

Inputs

- System description
- System security category
- System impact level
- NIST SP 800-53
- Organization catalog of common controls

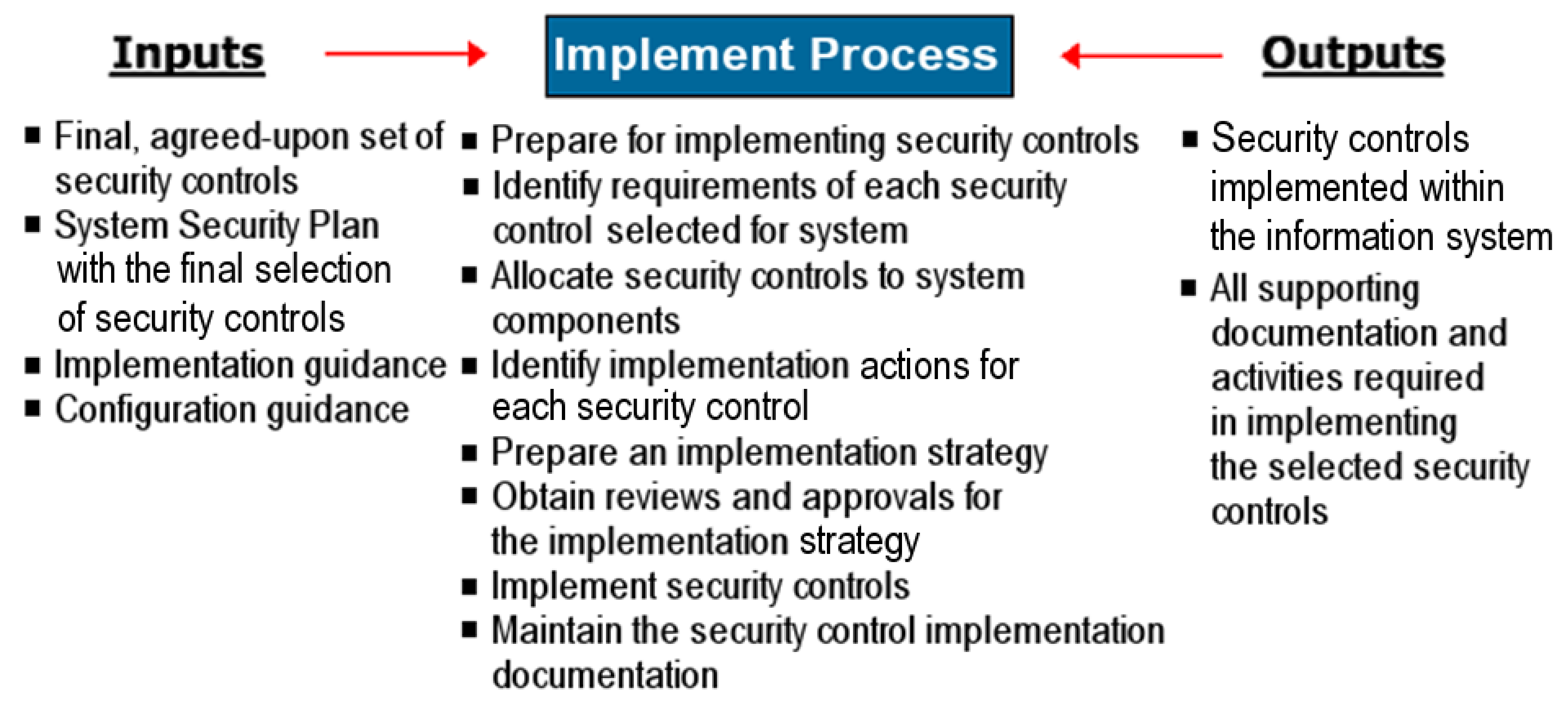
Select Process

- Prepare for selecting security controls
- Select initial security control baseline and minimum assurance requirements
- Apply scoping guidance
- Determine need for compensating controls
- Determine appropriate organization-defined values for identified parameters
- Supplement tailored security control baselines
- Determine if additional minimum assurance requirements are needed for moderate- and high-impact systems
- Document the selection decisions and update security plan
- Obtain approval of and agreement with security controls

Outputs

- Final, agreed-upon set of security controls

Implement Process



Inputs → **Implement Process** ← **Outputs**

Inputs

- Final, agreed-upon set of security controls
- System Security Plan with the final selection of security controls
- Implementation guidance
- Configuration guidance

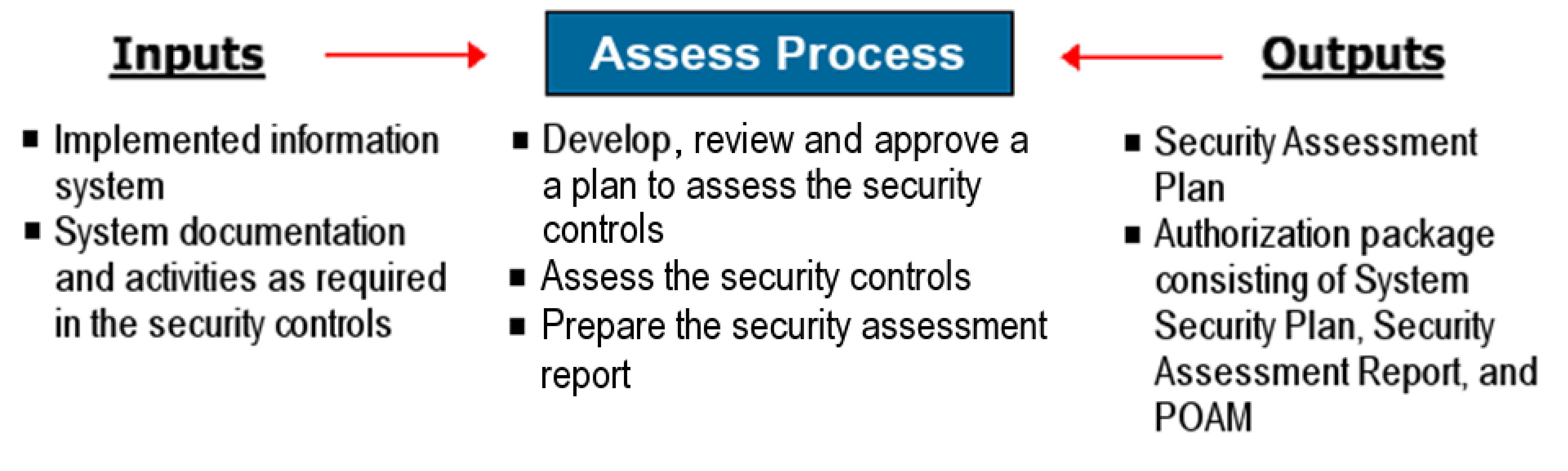
Implement Process

- Prepare for implementing security controls
- Identify requirements of each security control selected for system
- Allocate security controls to system components
- Identify implementation actions for each security control
- Prepare an implementation strategy
- Obtain reviews and approvals for the implementation strategy
- Implement security controls
- Maintain the security control implementation documentation

Outputs

- Security controls implemented within the information system
- All supporting documentation and activities required in implementing the selected security controls

Assess Process



Inputs → **Assess Process** ← **Outputs**

Inputs

- Implemented information system
- System documentation and activities as required in the security controls

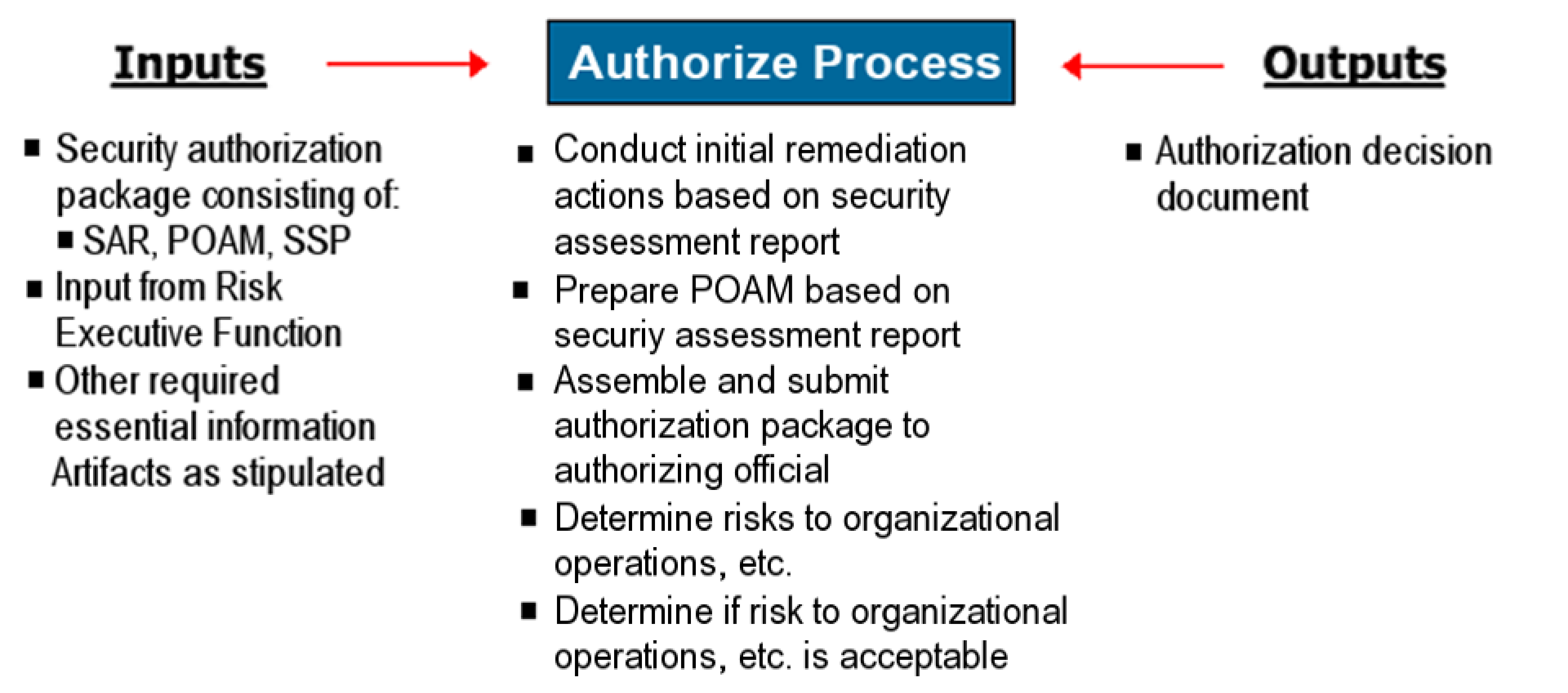
Assess Process

- Develop, review and approve a a plan to assess the security controls
- Assess the security controls
- Prepare the security assessment report

Outputs

- Security Assessment Plan
- Authorization package consisting of System Security Plan, Security Assessment Report, and POAM

Authorize Process



Inputs → **Authorize Process** ← **Outputs**

Inputs

- Security authorization package consisting of:
  - SAR, POAM, SSP
- Input from Risk Executive Function
- Other required essential information Artifacts as stipulated

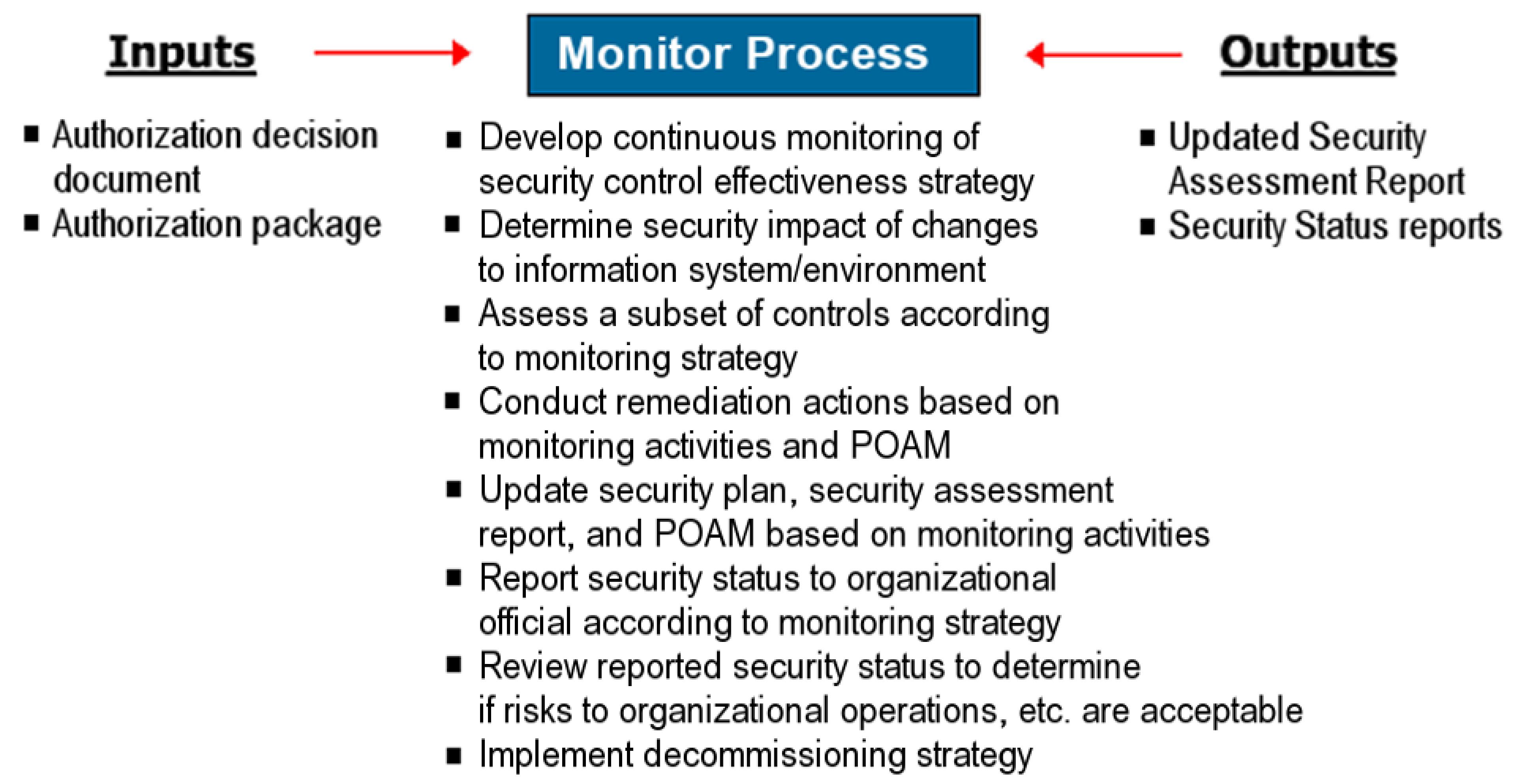
Authorize Process

- Conduct initial remediation actions based on security assessment report
- Prepare POAM based on securiy assessment report
- Assemble and submit authorization package to authorizing official
- Determine risks to organizational operations, etc.
- Determine if risk to organizational operations, etc. is acceptable

Outputs

- Authorization decision document

Monitor Process



Inputs → **Monitor Process** ← **Outputs**

Inputs

- Authorization decision document
- Authorization package

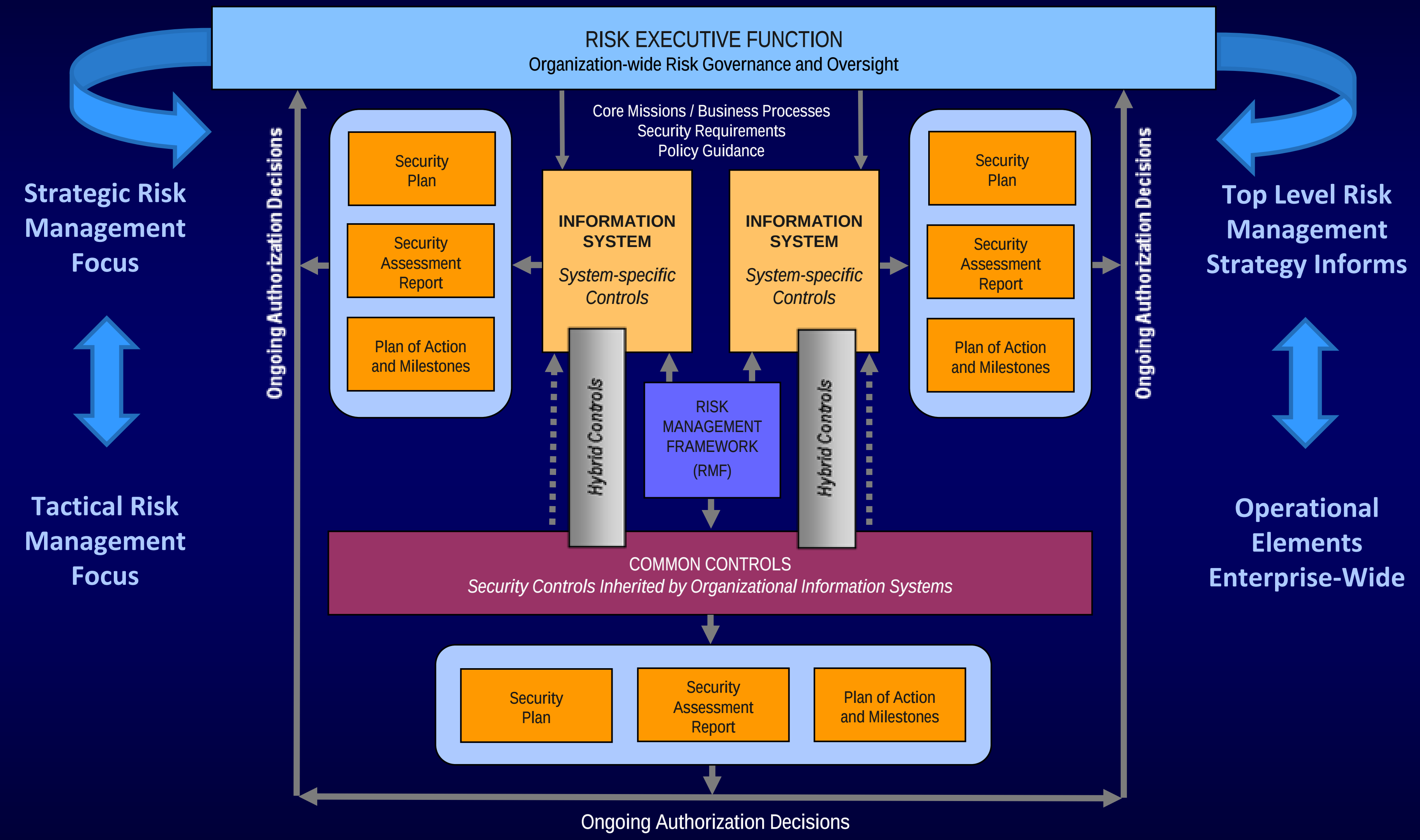
Monitor Process

- Develop continuous monitoring of security control effectiveness strategy
- Determine security impact of changes to information system/environment
- Assess a subset of controls according to monitoring strategy
- Conduct remediation actions based on monitoring activities and POAM
- Update security plan, security assessment report, and POAM based on monitoring activities
- Report security status to organizational official according to monitoring strategy
- Review reported security status to determine if risks to organizational operations, etc. are acceptable
- Implement decommissioning strategy

Outputs

- Updated Security Assessment Report
- Security Status reports

Security Control Allocation


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
Ongoing Authorization Decisions
Ongoing Authorization Decisions
Core Missions / Business Processes
Security Requirements
Policy Guidance
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
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

References

Joint Task Force Transformation Initiative

Core Risk Management Publications

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

- NIST Special Publication 800-37, Revision 1
  Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach
  ☑ *Completed*

- NIST Special Publication 800-53A, Revision 1
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
  Projected June 2010

Joint Task Force Transformation Initiative

Core Risk Management Publications

- NIST Special Publication 800-39

  Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View

  Projected November 2010

- NIST Special Publication 800-30, Revision 1

  Guide for Conducting Risk Assessments

  Projected November 2010

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