Information Systems Under Attack

Managing Enterprise Risk in Today's World of Sophisticated Threats and Adversaries

July 2, 2008

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The Current Landscape

- Public and private sector enterprises today are *highly dependent* on information systems to carry out their missions and business functions.
- To achieve mission and business success, enterprise information systems must be *dependable* in the face of serious cyber threats.
- To achieve information system dependability, the systems must be appropriately *protected*.

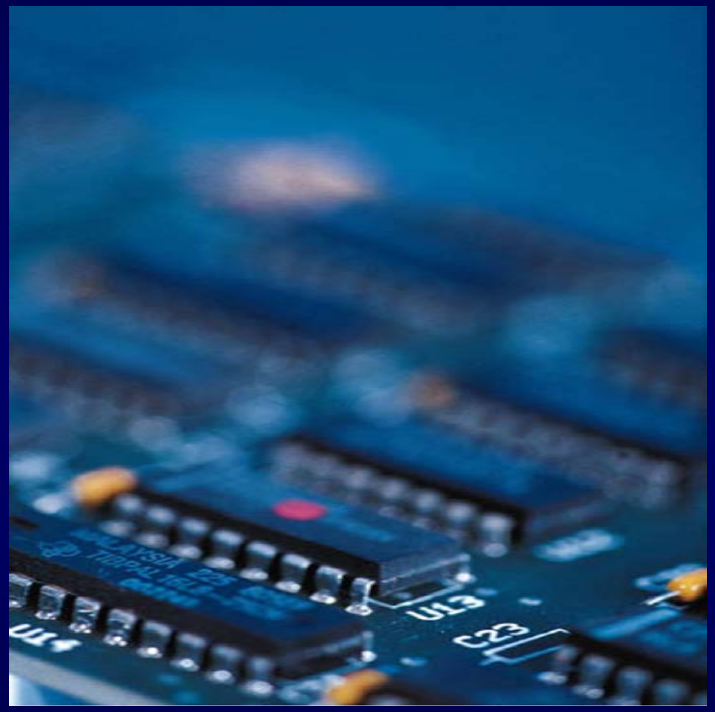
The Threat Situation

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.
- Significant exfiltration of critical and sensitive information and implantation of malicious software.

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 Defense, Civil, and Intelligence agencies within the federal government.
- 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

U.S. Critical Infrastructures

- "...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

  -- *USA Patriot Act (P.L. 107-56)*

Critical Infrastructure Protection

- The U.S. critical infrastructures are over 90% owned and operated by the private sector.
- Critical infrastructure protection must be a partnership between the public and private sectors.
- Information security solutions must be broad-based, consensus-driven, and address the ongoing needs of government and industry.

A National Imperative

For economic and national security reasons, we need—

- State-of-the-art cyber defenses for public and private sector enterprises.
- Adequate security for organizational operations (mission, functions, image, and reputation), organizational assets, individuals, other organizations (in partnership with the organization), and the Nation.
- A process for managing cyber risks in a dynamic environment where threats, vulnerabilities, missions, information systems, and operational environments are constantly changing.

Risk-Based Protection Strategy

- Enterprise missions and business processes drive security requirements and associated safeguards and countermeasures for organizational information systems.
- Highly flexible implementation; recognizing diversity in mission/ 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.

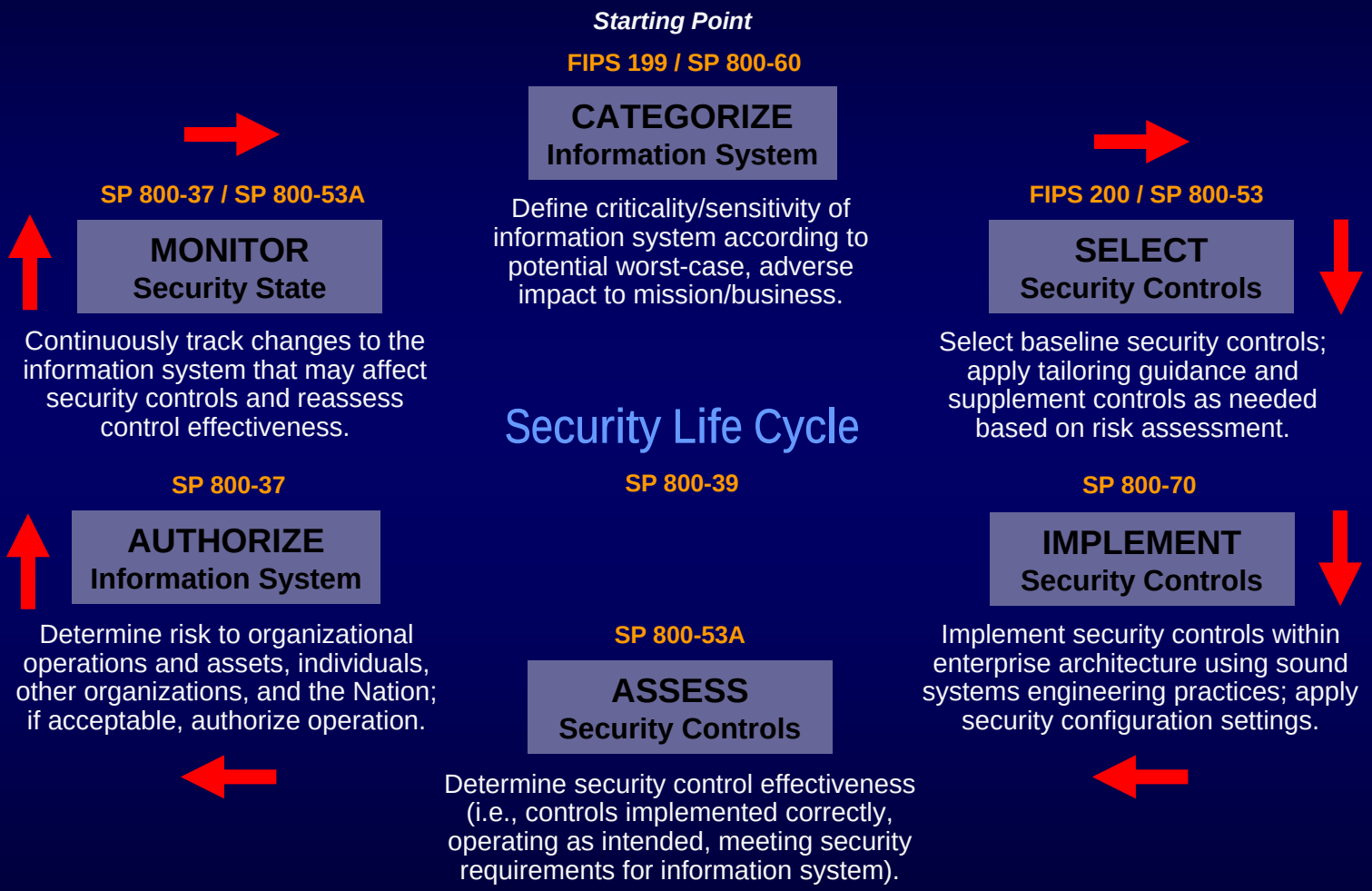
Information Security Programs

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

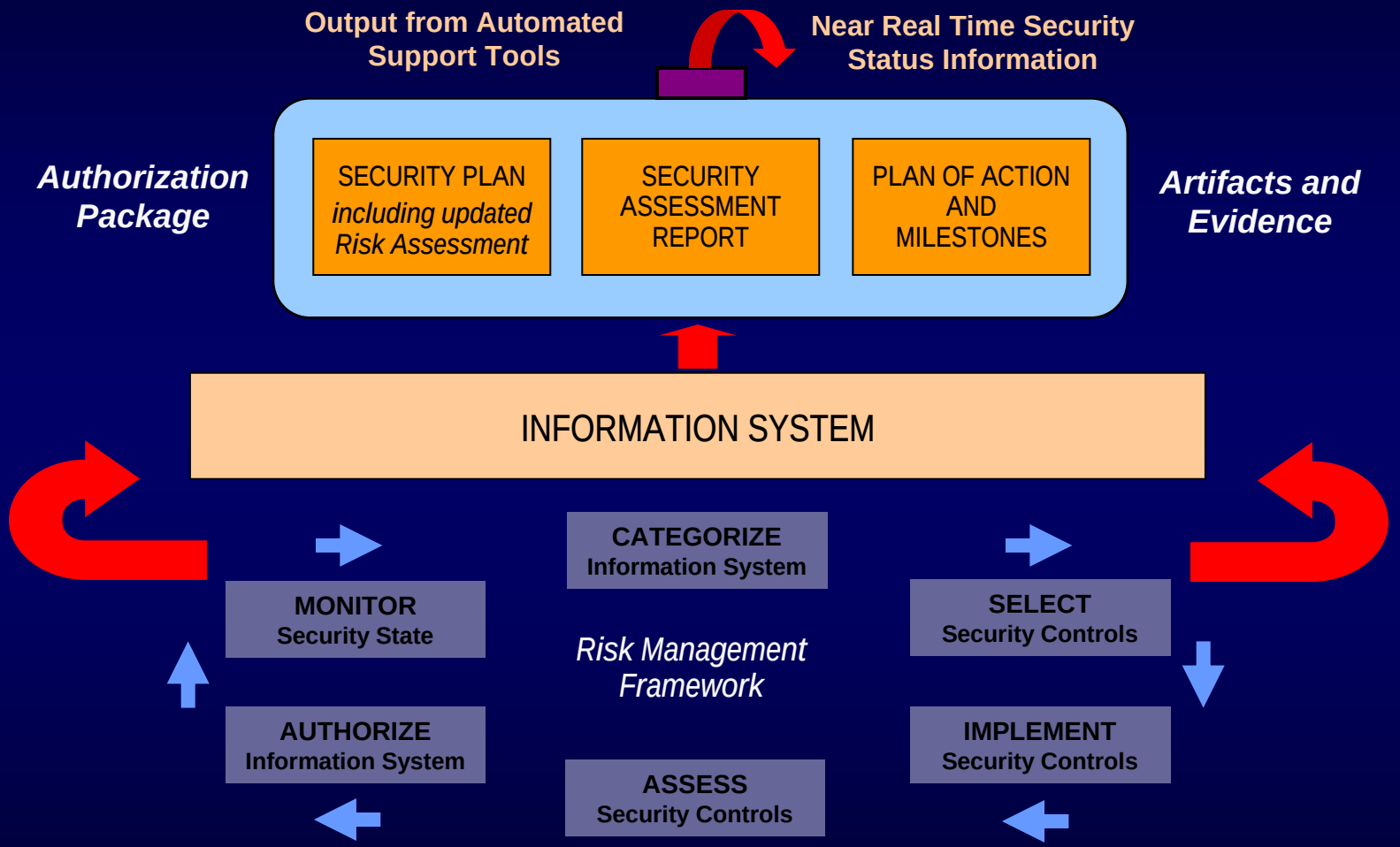
- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification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

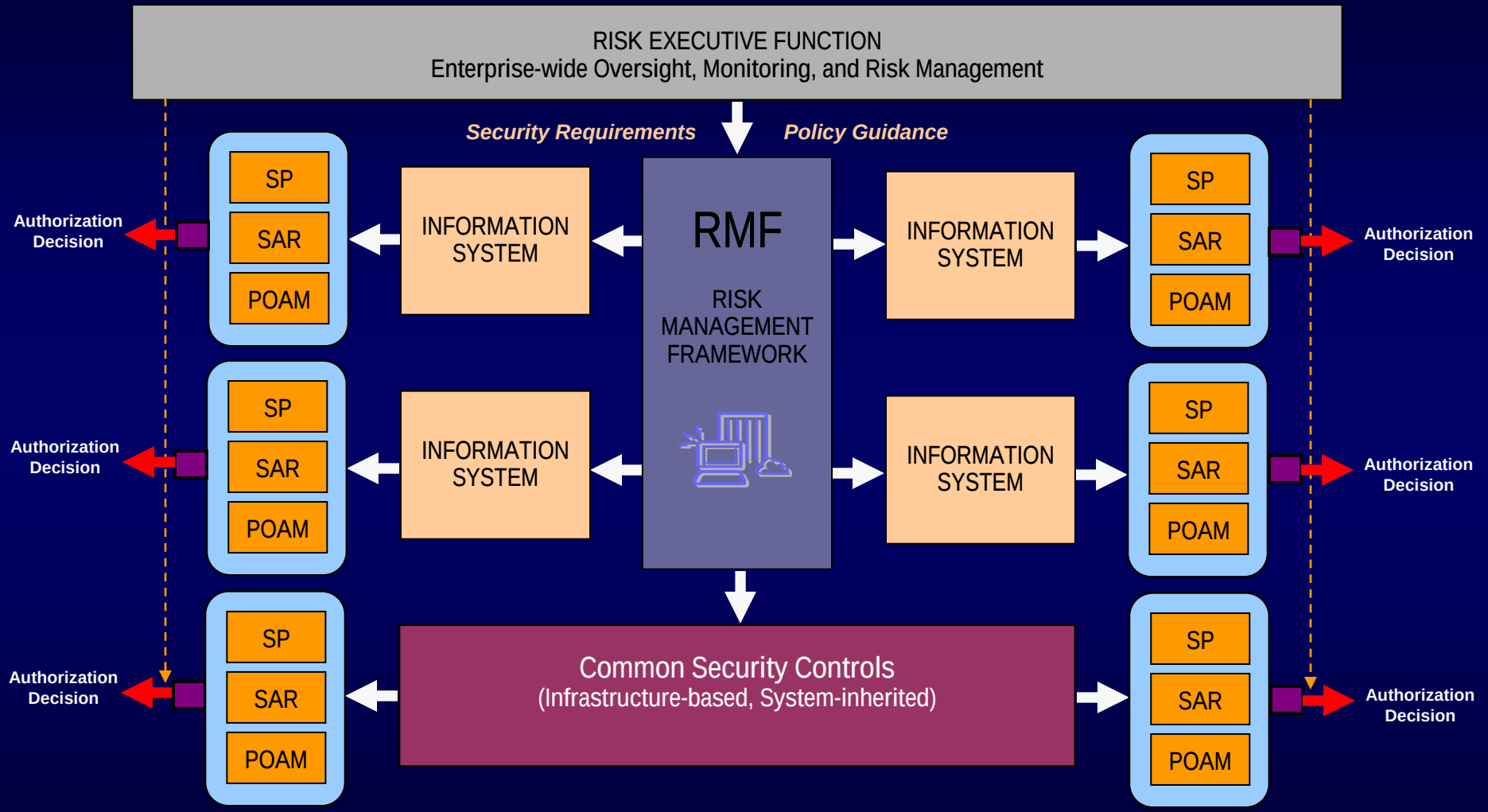
Risk Management Framework



Applying the Risk Management Framework to Information Systems



Extending the Risk Management Framework to Organizations



The Need for Trust Relationships

Changing ways we are doing business…

- Outsourcing
- Service Oriented Architectures
- Software as a Service
- Business Partnerships
- Information Sharing

Trustworthy Information Systems

- Trustworthy information systems are systems that are worthy of being trusted to operate within defined levels of *risk* to organizational operations and assets, individuals, other organizations, or the Nation despite:
  - *environmental disruptions*
  - *human errors*
  - *purposeful attacks*

  that are expected to occur in the specified environments of operation.

Information System Trustworthiness

- Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the *confidentiality*, *integrity*, and *availability* of the information being processed, stored, or transmitted by the system.
- Trustworthiness defines the *security state* of the information system at a particular point in time and is *measurable*.

Information System Trustworthiness

Two factors affecting the trustworthiness of information systems include:

- *Security functionality* (i.e., the security-related features or functions employed within an information system or the infrastructure supporting the system); and
- *Security assurance* (i.e., the grounds for confidence that the security functionality, when employed within an information system or its supporting infrastructure, is effective in its application).

Elements of Trust

Trust among partners can be established by:

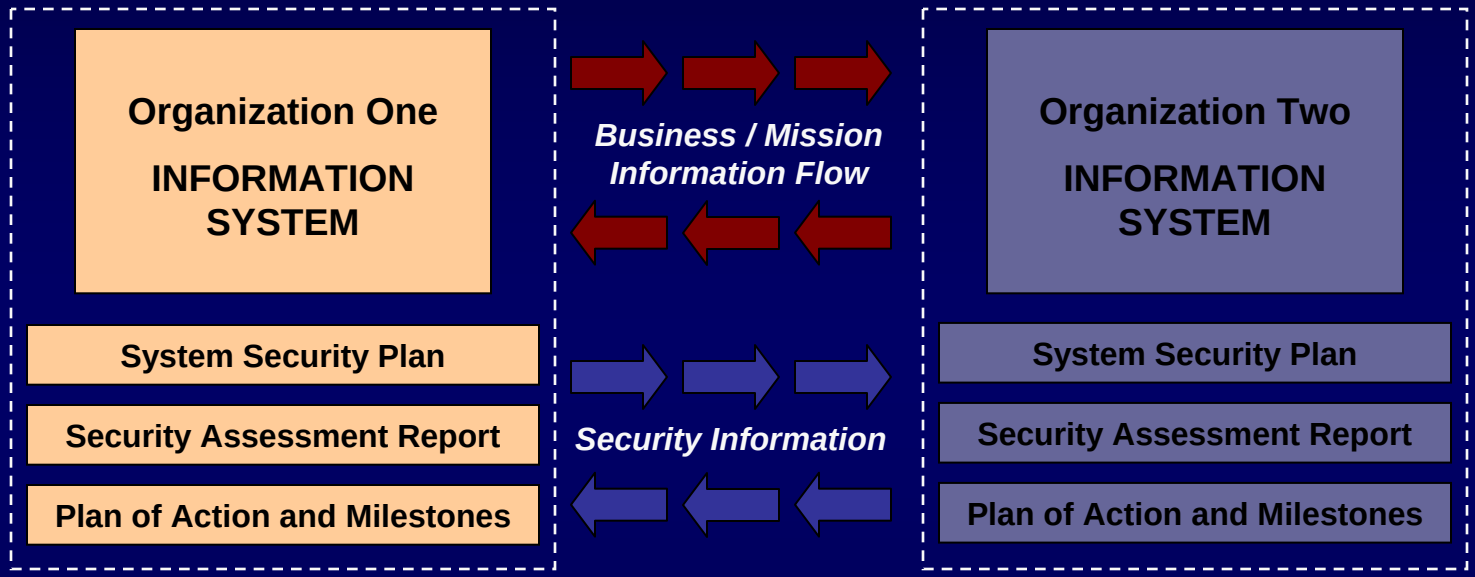
- Identifying the goals and objectives for the provision of services/information or information sharing;
- Agreeing upon the risk from the operation and use of information systems associated with the provision of services/information or information sharing;
- Agreeing upon the degree of trustworthiness (i.e., the security functionality and assurance) needed for the information systems processing, storing, or transmitting shared information or providing services/information in order to adequately mitigate the identified risk;
- Determining if the information systems providing services/information or involved in information sharing activities are worthy of being trusted; and
- Providing ongoing monitoring and management oversight to ensure that the trust relationship is maintained.

The Trust Continuum

- Trust relationships among partners can be viewed as a continuum—ranging from a high degree of trust to little or no trust…
- The degree of trust in the information systems supporting the partnership should be factored into risk decisions.

Trust Relationships

Security Visibility Among Mission/Business Partners

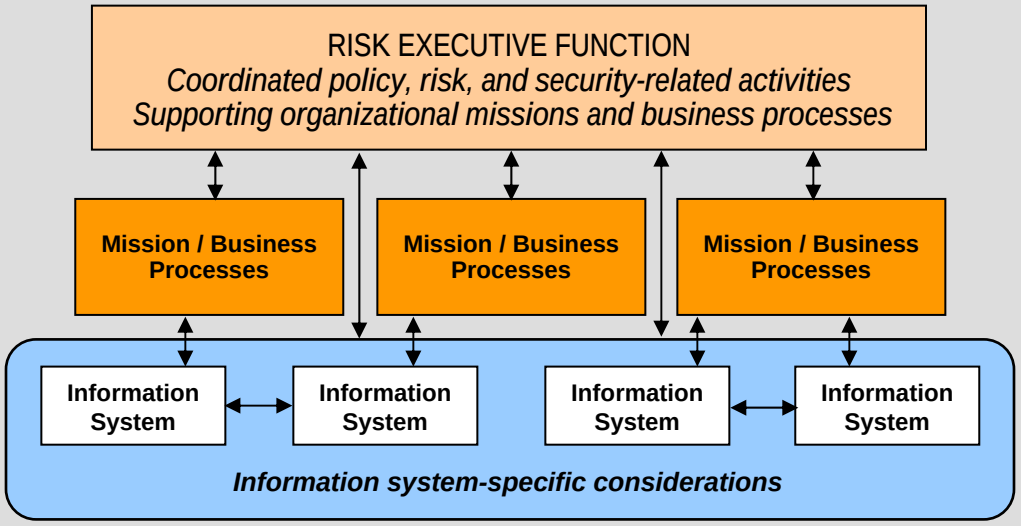


Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

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 *visibility* into prospective mission/business partners information security programs…establishing a trust relationship based on the trustworthiness of information systems.

Risk Executive Function



- Establish organizational information security priorities.
- Allocate information security resources across the organization.
- Provide oversight of information system security categorizations.
- Identify and assign responsibility for common security controls.
- Provide guidance on security control selection (tailoring and supplementation).
- Define common security control inheritance relationships for information systems.
- Establish and apply mandatory security configuration settings.
- Identify and correct systemic weaknesses and deficiencies in information systems.

Strategic Planning Considerations

- Consider vulnerabilities of new information technologies and system integration before deployment.
- Diversify information technology assets.
- Reduce information system complexity.
- Apply a balanced set of management, operational, and technical security controls in a defense-in-depth approach.
- Detect and respond to breaches of information system boundaries.
- Reengineer mission/business processes.

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

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 certification and accreditation process

National security and non national security information systems

ISO 27001 Harmonization Initiative

- Define relationship between the FISMA security standards and guidelines and the ISO 27001 Information Security Management System.
- Provide comprehensive mapping from FISMA standards and guidelines to ISO 27001.
- Develop and publish a “delta document” that states commonalities and differences among the standards.
- Explore possibilities for recognition and acceptance of assessment results to reduce information security costs.

The Golden Rules

Building an Effective Enterprise Information Security Program

- Develop an enterprise-wide information security strategy and game plan.
- Get corporate “buy in” for the enterprise information security program—effective programs start at the top.
- Build information security into the infrastructure of the enterprise.
- Establish level of “due diligence” for information security.
- Focus initially on mission/business process impacts—bring in threat information only when specific and credible.

The Golden Rules

Building an Effective Enterprise Information Security Program

- Create a balanced information security program with management, operational, and technical security controls.
- Employ a solid foundation of security controls first, then build on that foundation guided by an assessment of risk.
- Avoid complicated and expensive risk assessments that rely on flawed assumptions or unverifiable data.
- Harden the target; place multiple barriers between the adversary and enterprise information systems.

The Golden Rules

Building an Effective Enterprise Information Security Program

- Be a good consumer—beware of vendors trying to sell single point solutions for enterprise security problems.
- Don't be overwhelmed with the enormity or complexity of the information security problem—take one step at a time and build on small successes.
- Don't tolerate indifference to enterprise information security problems.

And finally…

- Manage enterprise risk—don't try to avoid it!

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

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

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

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

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov