

Managing Risk in New Computing Paradigms

Applying FISMA Standards and Guidelines to Cloud Computing

SaaS/Gov 2009

February 25, 2009

Dr. Ron Ross

*Computer Security Division
Information Technology Laboratory*

The Threat Situation

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

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.

External Service Providers

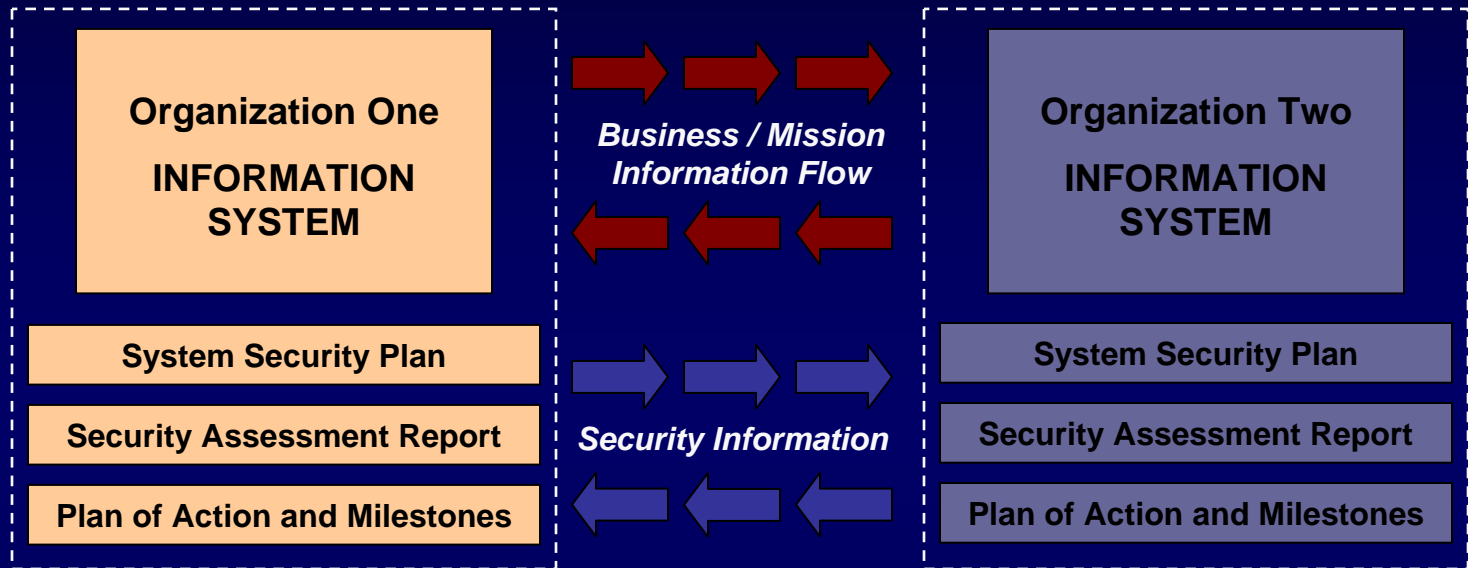
- Organizations are becoming increasingly reliant on information system services provided by external service providers to carry out important missions and functions.
- Organizations have varying degrees of control over external service providers.
- Organizations must establish trust relationships with external service providers to ensure the necessary security controls are in place and are effective in their application.
- Where control of external service providers is limited or infeasible, the organization factors that situation into its risk assessment.

The Need for Trust Relationships

Changing ways we are doing business...

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

Trust Relationships



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 and *understanding* of prospective partner's information security programs...establishing a trust relationship based on the trustworthiness of their information systems.

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*.

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.



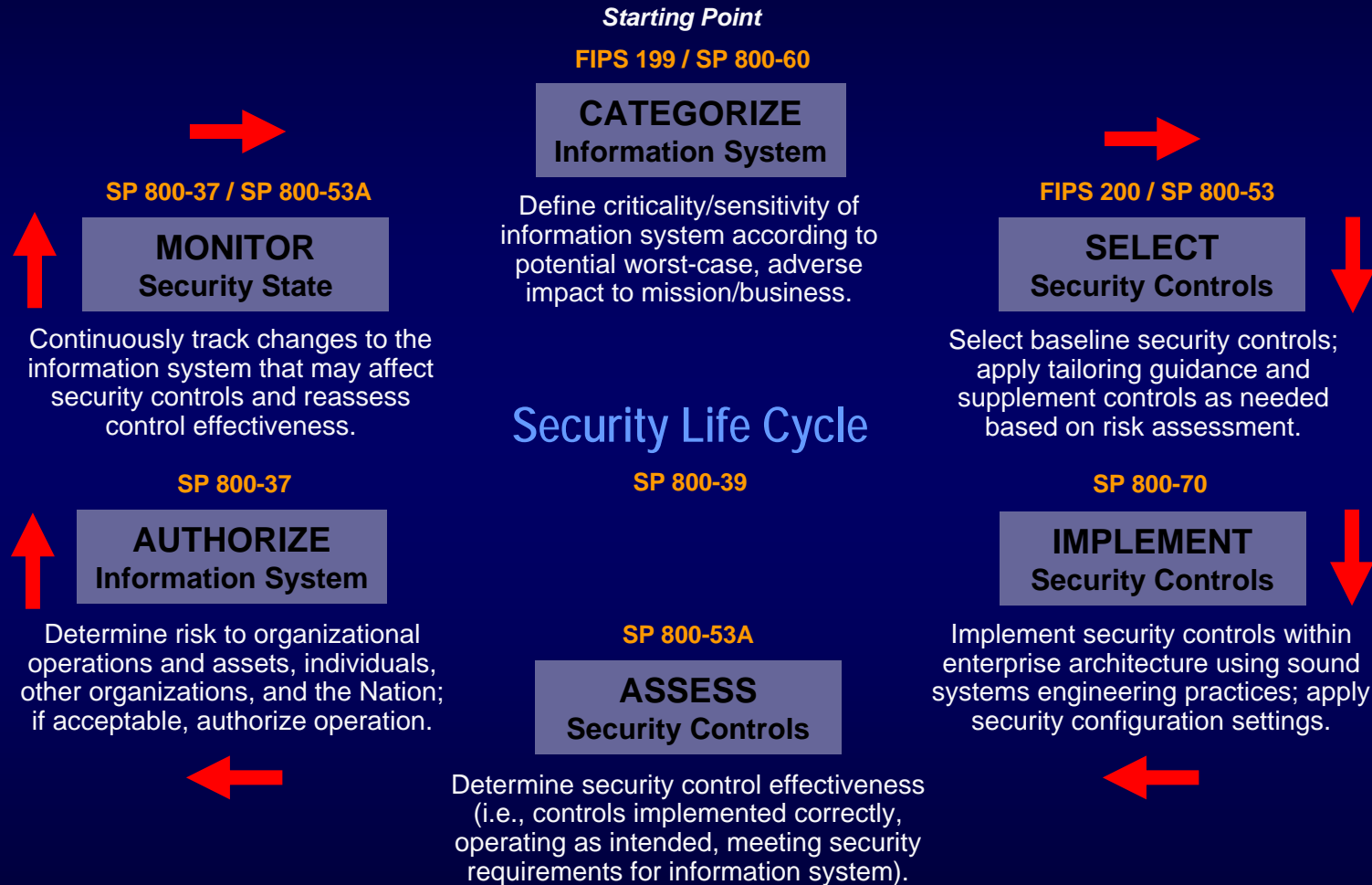
Information Security Programs

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

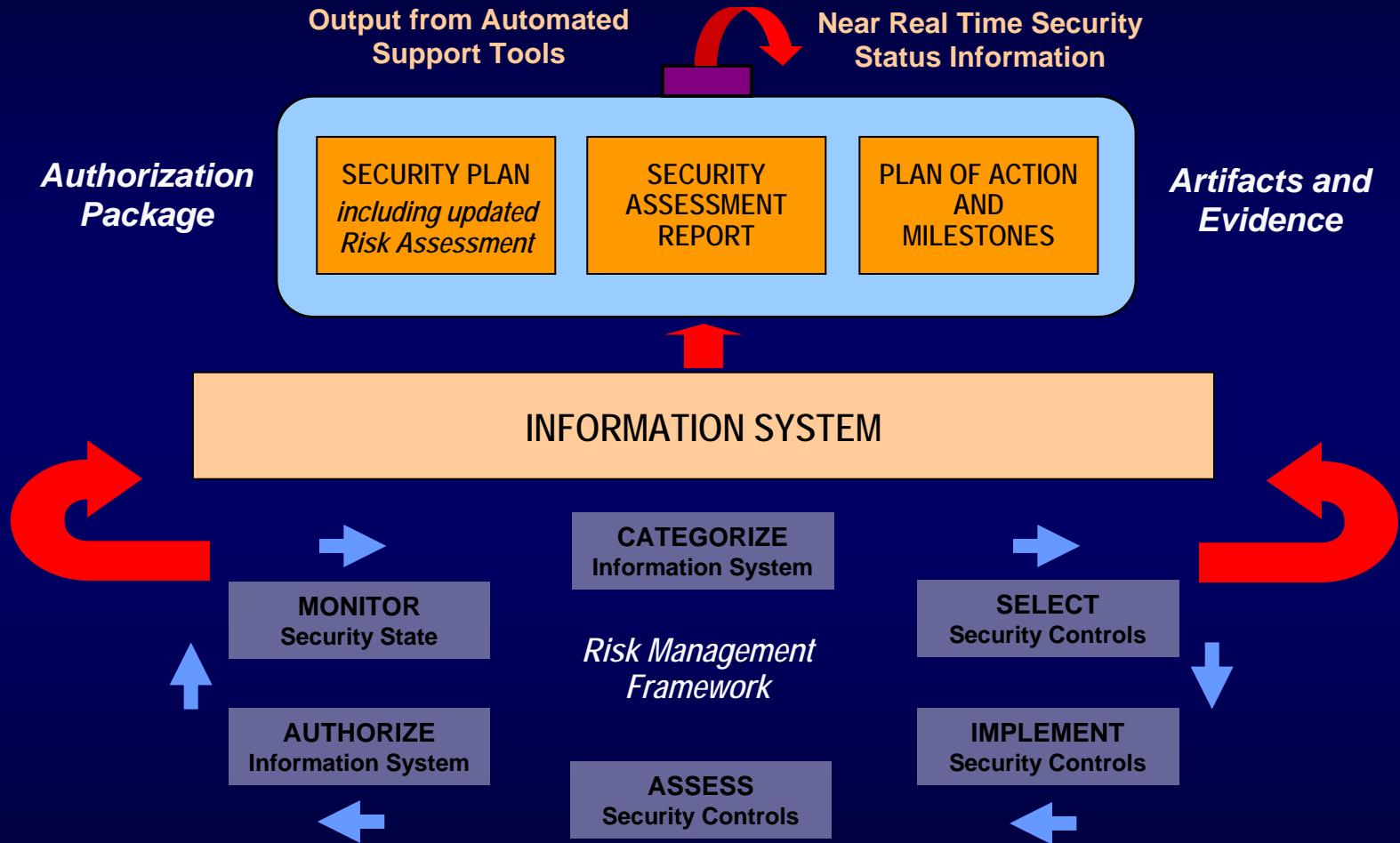
- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification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



Security Authorization

- An inherent federal responsibility carried out by a senior management official.
- Different models of security authorizations:
 - Single agency authorization;
 - Single agency authorization on behalf of multiple agencies;
 - Joint authorization by multiple agencies.
- Economies of scale.
- Reuse of authorization information.

Some Provider Challenges

- In an environment serving multiple customers with different security needs, what is a sufficient level of protection?
 - High water mark?
 - Meeting the security requirements of the most demanding customer?
- How to provide appropriate evidence of security due diligence.

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