Near Real Time Risk Management

Transforming the Certification and Accreditation Process

Information Security and Privacy Advisory Board

June 6, 2008

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

The last line of defense for ensuring that —

- Adequate safeguards and countermeasures are employed within information systems and supporting infrastructures.
- Information system safeguards and countermeasures are effective in their application.
- Risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is explicitly understood and accepted by leaders at all levels.
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
Transforming the C&A Process

- Describe the C&A process in terms of the Risk Management Framework and change the focus of the process from a static event—

  ...to a more dynamic, near real time, information system monitoring process carried out with automated support tools as part of an enterprise risk management process.

- Extend the Risk Management Framework from individual information systems to the enterprise—

  ...to provide a corporate-wide perspective on managing risk from information systems and the complex missions and business functions supported by those systems.
Transforming the C&A Process

- Incorporate a trust model into risk management activities—
  ...to address partnerships, information sharing, new computing paradigms, and methods of operation (e.g., common security controls, joint authorizations, external service providers, shared services, outsourcing, service-oriented architectures, software-as-a-service).

- Integrate the Risk Management Framework into the organization’s Enterprise Architecture and System Development Life Cycle—
  ...to ensure information security requirements are tightly coupled into the system design and development processes and to take maximum advantage of ongoing life cycle activities including reuse of assessment results and documentation (i.e., artifacts and evidence).
Transformation #1

Reflecting the C&A Process within the Risk Management Framework
Current C&A Process

- Initiation Phase
- Certification Phase
- Accreditation Phase
- Continuous Monitoring Phase

*Expressed within the context of the Risk Management Framework as follows...*
**Risk Management Framework Steps 1 through 3**

**Initiation Phase**

**FIPS 199 / SP 800-60**

**CATEGORIZE Information System**

- Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

**SP 800-37 / SP 800-53A**

**MONITOR Security Controls**

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

**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 800-39**

**AUTHORIZE Information System**

- Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

**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).
Certification Phase
Risk Management Framework Step 4

Starting Point
FIPS 199 / SP 800-60

CATEGORIZE
Information System

SP 800-37
SP 800-53A

MONITOR
Security Controls

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 199 / SP 800-60

AUTHORIZE
Information System

SP 800-37

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

FIPS 199 / SP 800-60

SELECT
Security Controls

SP 800-53A

IMPLEMENT
Security Controls

SP 800-70

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37

ASSESS
Security Controls

SP 800-39

SELECT
Security Controls

FIPS 200 / SP 800-53

MONITOR
Security Controls

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

FIPS 199 / SP 800-60

SP 800-37

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 199 / SP 800-60

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

FIPS 199 / SP 800-60

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

FIPS 200 / SP 800-53

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.
Accreditation Phase

Risk Management Framework Step 5

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.

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

SP 800-39

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

FIPS 200 / SP 800-53

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 199 / SP 800-60

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.

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

SP 800-39

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

FIPS 200 / SP 800-53

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 199 / SP 800-60

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.

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

SP 800-39

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

FIPS 200 / SP 800-53

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 199 / SP 800-60

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.

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

SP 800-39

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-70

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-53A

SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

FIPS 200 / SP 800-53

MONITOR Security Controls

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

SP 800-37 / SP 800-53A

CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.
Continuous Monitoring Phase

Risk Management Framework Step 6

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.

MONITOR Security Controls
SP 800-37 / SP 800-53A
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

AUTHORIZE Information System
SP 800-37
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

ASSESS Security Controls
SP 800-53A
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

Security Life Cycle
SP 800-39

IMPLEMENT Security Controls
SP 800-70
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.
Transformation #2

Extending the Risk Management Framework to the Enterprise
Applying the Risk Management Framework to Information Systems

Output from Automated Support Tools

Authorization Package

SECURITY PLAN including updated Risk Assessment

SECURITY ASSESSMENT REPORT

PLAN OF ACTION AND MILESTONES

Near Real Time Security Status Information

Artifacts and Evidence

INFORMATION SYSTEM

MONITOR Security Controls

CATEGORIZE Information System

SELECT Security Controls

IMPLEMENT Security Controls

AUTHORIZE Information System

ASSESS Security Controls

Risk Management Framework

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Extending the Risk Management Framework to Organizations

RISK EXECUTIVE FUNCTION
Enterprise-wide Oversight, Monitoring, and Risk Management

Security Requirements → Policy Guidance

Authorization Decision

INFORMATION SYSTEM

RMF
RISK MANAGEMENT FRAMEWORK

Common Security Controls (Infrastructure-based, System-inherited)

INFORMATION SYSTEM

INFORMATION SYSTEM

INFORMATION SYSTEM

INFORMATION SYSTEM

Authorization Decision

Authorization Decision

Authorization Decision

Authorization Decision

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Managing Risk at the Organizational Level

- 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.
Transformation #3

Incorporating Trust Models into Enterprise Risk Management
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

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.
Transformation #4

Integrating Risk Management into Enterprise Architectures and System Development Life Cycle Processes
Main Streaming Information Security

- Information security requirements must be considered first order requirements and are critical to mission and business success.

- An effective organization-wide information security program helps to ensure that security considerations are specifically addressed in the enterprise architecture for the organization and are integrated early into the system development life cycle.
Enterprise Architecture

- Provides a common language for discussing information security in the context of organizational missions, business processes, and performance goals.

- Defines a collection of interrelated reference models that are focused on lines of business including Performance, Business, Service Component, Data, and Technical.

- Uses a security and privacy profile to describe how to integrate the Risk Management Framework (including the embedded C&A process) into the reference models.
System Development Life Cycle

- The Risk Management Framework (including the embedded C&A process) should be integrated into all phases of the SDLC.
  - Initiation (RMF Steps 1 and 2)
  - Development and Acquisition (RMF Step 2)
  - Implementation (RMF Steps 3 through 5)
  - Operations and Maintenance (RMF Step 6)
  - Disposition (RMF Step 6)

- Reuse system development artifacts and evidence (e.g., design specifications, system documentation, testing and evaluation results) for risk management activities including C&A.
FISMA Phase I Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) *
- NIST Special Publication 800-39 (Risk Management) **
- NIST Special Publication 800-37 (Certification & Accreditation) *
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment) **
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping) *

* Publications currently under revision.
** Publications currently under development.
Final Phase I Projects

- Publication of NIST Special Publication 800-39
- Completion of NIST Special Publication 800-53A
- Revision of NIST Special Publication 800-37
- Revision of NIST Special Publication 800-30
- Publication of an Authorizing Official’s Handbook
- Publication of Configuration Management Guideline
- Publication of Industrial Control System Security Control Augmentations
FISMA Phase II
FISMA Phase II

- **Mission:** Develop and implement a standards-based organizational credentialing program for public and private sector entities to demonstrate core competencies for offering security services to federal agencies.

- **Timeline:** 2007-2010

- **Status:** Initial work started in late 2007.
FISMA Phase II

Demonstrating competence to provide information security services including—

- Assessments of Information Systems
  (Operational environments)
  - Security controls and assurances
  - Configuration settings

- Assessments of Information Technology Products/Services
  (Laboratory environments)
  - Security functionality (features) and assurances
  - Configuration settings
Producing evidence that supports the grounds for confidence in the design, development, implementation, and operation of information systems.
FISMA Phase II Project Initiatives

- Organizational Credentialing Initiative
- Product and Service Supplier Assurance Initiatives
- Support Tools, Techniques, Reference Materials, Practices & Validation Program Initiatives
- Training Initiative
- ISO Harmonization Initiative
Organizational Credentialing Initiative


- Draft Criteria for Product & Service Supplier Claims Statement
Training Initiative

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards and guidelines.

- Training initiative includes three components—
  - Frequently Asked Questions
  - Publication Summary Guides (Quickstart Guides)
  - Formal Curriculum and Training Courses

- NIST will provide initial training in order to fine-tune the curriculum; then transition to other providers.
ISO 27001 Harmonization Initiative


- 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.
FISMA Phase II

Near Term Tasks and Milestones

- Update Draft NISTIR 7328 based on public comments (August 2008).
- FISMA FAQ’s (initial draft August 2008).
- Draft criteria, structure, guidelines, etc. for products and services claiming support of 800-53 security controls (September 2008).
- Initial Risk Management Framework training module — Categorize Step (September 2008).
- FISMA Phase II workshop (October 2008).
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: csrm.nist.gov/sec-cert
Comments: sec-cert@nist.gov