Risk Management Framework

Computer Security Division
Information Technology Laboratory
Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk resulting from the operation of an information system:
  - ✔ **Categorize** the information system
  - ✔ **Select** set of minimum (baseline) security controls
  - ✔ **Refine** the security control set based on risk assessment
  - ✔ **Document** security controls in system security plan
  - ✔ **Implement** the security controls in the information system
  - ✔ **Assess** the security controls
  - ✔ **Determine** agency-level risk and risk acceptability
  - ✔ **Authorize** information system operation
  - ✔ **Monitor** security controls on a continuous basis
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.

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

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

MONITOR Security State
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Controls)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-37 (System Risk Management Framework)
- NIST Special Publication 800-39 (Enterprise-Wide Risk Management)
- 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)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation...
# Information Security Program

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

<table>
<thead>
<tr>
<th>Management</th>
<th>Operational</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>Access control mechanisms</td>
<td></td>
</tr>
<tr>
<td>Security planning</td>
<td>Identification &amp; authentication mechanisms</td>
<td></td>
</tr>
<tr>
<td>Security policies and procedures</td>
<td>(Biometrics, tokens, passwords)</td>
<td></td>
</tr>
<tr>
<td>Contingency planning</td>
<td>Audit mechanisms</td>
<td></td>
</tr>
<tr>
<td>Incident response planning</td>
<td>Encryption mechanisms</td>
<td></td>
</tr>
<tr>
<td>Security awareness and training</td>
<td>Firewalls and network security mechanisms</td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td>Intrusion detection systems</td>
<td></td>
</tr>
<tr>
<td>Personnel security</td>
<td>Security configuration settings</td>
<td></td>
</tr>
<tr>
<td>Certification, accreditation, and security assessments</td>
<td>Anti-viral software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smart cards</td>
<td></td>
</tr>
</tbody>
</table>

Adversaries attack the weakest link…where is yours?

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Security Control Accountability

RISK EXECUTIVE FUNCTION
Organization-wide Risk Governance and Oversight

Core Missions / Business Processes
Security Requirements
Policy Guidance

INFORMATION SYSTEM
System-specific Controls

Security Plan
Security Assessment Report
Plan of Action and Milestones

RISK MANAGEMENT FRAMEWORK (RMF)

COMMON CONTROLS
Security Controls Inherited by Organizational Information Systems

Security Plan
Security Assessment Report
Plan of Action and Milestones

Top Level Risk Management Strategy Informs
Operational Elements Enterprise-Wide

Strategic Risk Management Focus
Tactical Risk Management Focus

Ongoing Authorization Decisions
The Desired End State

*Security Visibility Among Business/Mission Partners*

**Organization One**

- Information System
- System Security Plan
- Security Assessment Report
- Plan of Action and Milestones

**Organization Two**

- Information System
- System Security Plan
- Security Assessment Report
- Plan of Action and Milestones

Determining the risk to the first organization’s operations and assets and the acceptability of such risk

Determining the risk to the second organization’s operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin…establishing levels 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

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

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

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

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