Risk Management Guide for Information Technology Systems

NIST SP800-30
Overview
Risk Management

- Process that allows IT managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting IT systems and data that support organizations’ missions.
- An iterative process that can be performed during each major SDLC phase
Effective risk management must be totally integrated into the SDLC.

Five SDLC phases:
1. Initiation
2. Development or acquisition
3. Implementation
4. Operation or maintenance
5. Disposal.

Enterprise security requires that everyone understand their roles
Key Roles One

Senior management

- Under due care, ultimately responsibility for mission accomplishment
- Must ensure that necessary resources are effectively applied to develop capabilities needed to accomplish mission.

Chief Information Officer (CIO).

- Responsible for the agency’s IT planning, budgeting, and performance including its information security components.

System and Information Owners.

- Responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own.
Key Roles Two

Business and Functional Managers
- Responsible for business operations and IT procurement process.
- Must take active role in the risk management process.
- Individuals with authority and responsibility for making trade-off decisions essential to mission accomplishment.

ISSO
- IT security program managers and computer security officers responsible for their organizations’ security programs.

IT Security Practitioners
- IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems.

Users
- Use IT systems and data according to an organization’s policies, guidelines, and rules of behavior.
Risk Management Methodology

...Identifies appropriate controls that provide mission-essential security capabilities.

Encompasses three related processes

1. Risk Assessment
2. Risk Mitigation
3. Evaluation and Assessment
Risk Assessment Process

- Risk is a function of the likelihood of a given threat-source exercising a particular vulnerability as well as the resulting adverse impact on the organization.

Organizational risk assessment identifies:

1. Vulnerabilities
2. Threats
3. Associated risks.
   - Also identifies appropriate risk mitigation controls.
Nine Risk Assessment Steps (NIST)

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Note

Steps 2, 3, 4, 5, and 6, may be conducted in parallel.
Threats and Related Terms

Threat

Potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat-Source

1. intent and method targeted at the intentional exploitation of a vulnerability
2. Situation and method that may accidentally trigger a vulnerability.

Common Threat-Sources

Natural

- Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, other events.

Human

- Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).

Environmental

- Long-term power failure, pollution, chemicals, liquid leakage.
Flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.

- May be technical or nontechnical
- Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test).

Test methods include
  - Automated vulnerability scanning tool
  - Security test and evaluation (ST&E)
  - Penetration testing.
The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low.

Table 3-4. Likelihood Definitions

<table>
<thead>
<tr>
<th>Likelihood Level</th>
<th>Likelihood Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.</td>
</tr>
<tr>
<td>Medium</td>
<td>The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.</td>
</tr>
<tr>
<td>Low</td>
<td>The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.</td>
</tr>
</tbody>
</table>

Output from Step 5—Likelihood rating (High, Medium, Low)
Impact Analysis

Mission impact analysis (also known as business impact analysis [BIA]) prioritizes impact levels associated with the compromise of an organization’s information assets based on a qualitative or quantitative assessment of sensitivity and criticality of those assets.

- An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization’s critical missions.
## Risk Determination

### Table 3-7. Risk Scale and Necessary Actions

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk Description and Necessary Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.</td>
</tr>
<tr>
<td>Medium</td>
<td>If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.</td>
</tr>
<tr>
<td>Low</td>
<td>If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.</td>
</tr>
</tbody>
</table>

*Output from Step 7—Risk level (High, Medium, Low)*
Processes Flow

1. Risk Assessment
2. Risk Mitigation
3. Evaluation and Assessment

- Creates security posture snapshot.
  - Process is iterative
  - Current snapshot provide baseline for future snapshots
Seven (NSA) InfoSec Assessment Methodology (IAM) Steps

1. Categorize and Define Information
2. Identify System Boundaries
3. Collect Documents
4. Assessment Plan
5. Analyze INFOSec Posture
6. Exit Briefing
7. Analysis and Written Report
IAM, IEM, Red Team

ASSESSMENTS (Level I) → EVALUATIONS (Level II) → RED TEAM (Level III)
Input

• Risk levels from the risk assessment report

Risk Mitigation Activities

Step 1. Prioritize Actions

Step 2. Evaluate Recommended Control Options
• Feasibility
• Effectiveness

Step 3. Conduct Cost-Benefit Analysis
• Impact of implementing
• Impact of not implementing
• Associated costs

Step 4. Select Controls

Step 5. Assign Responsibility

Step 6. Develop Safeguard Implementation Plan
• Risks and Associated Risk Levels
• Prioritized Actions
• Recommended Controls
• Selected Planned Controls
• Responsible Persons
• Start Date
• Target Completion Date
• Maintenance Requirements

Step 7. Implement Selected Controls

Output

Actions ranking from High to Low

List of possible controls

Cost-benefit analysis

Selected Controls

List of responsible persons

Safeguard implementation plan

Residual Risks
Risk Mitigation Strategy

Figure 4-1. Risk Mitigation Action Points
Three Security Areas

1. Management
2. Operational
3. Technical

- AKA PPT
Management Security Domain

- Assignment of responsibilities
- Continuity of support
- Incident response capability
- Periodic security controls review
- Personnel clearance and background investigations
- Risk assessment
- Security and technical training
- Separation of duties
- System authorization and reauthorization
- System or application security plan
Operational Security Domain

- Air-borne contaminants control
  - Smoke, dust, chemicals
- Controls to ensure electrical power supply quality
- Data media access and disposal
- External data distribution and labeling
- Facility protection
  - e.g., computer room, data center, office
- Humidity and Temperature control
- Workstations, laptops, and stand-alone personal computers
Technical Security Domain

- Communications
  - e.g., dial-in, system interconnection, routers
- Cryptography
- Discretionary access control
- Identification and authentication
- Intrusion detection
- Object reuse
- System audit
Control Methods: Technical or Not

- Controls use technical and/or nontechnical methods.
  - Technical controls: safeguards incorporated into hardware, software, or firmware
    - e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software.
  - Nontechnical methods: management and operational controls
    - Security policies; operational procedures; and personnel, physical, and environmental security.
Control Categories

- Both technical and nontechnical control methods further categorized as preventive, detective, or restorative.
  - Preventive controls inhibit attempts to violate security policy
    - Access control enforcement, encryption, and authentication.
  - Detective controls warn of violations or attempted violations of security policy
    - Audit trails, intrusion detection methods, and checksums.
Control Categories

Technical
1. Support
2. Prevent
3. Detect and Recover

Management
1. Preventive
2. Detection
3. Recovery

Operational
1. Preventative
2. Detective
Eighteen Baseline INFOSEC Classes in Three Categories

Management
- INFOSEC documentation
- INFOSEC roles and responsibilities
- Contingency planning
- Configuration Management

Operational
- Media controls
- Physical environment
- Personnel security
- Education, training, and awareness

Technical
- Identification and authentication
- Account management
- Session controls
- Auditing
- Malicious code protection
- Maintenance
- System assurance
- Networking/connectivity
- Communications security
Figure 4-3. Technical Security Controls
Supporting Technical Controls

- Identification
- Cryptographic Key Management
- Security Administration
- System Protections
Preventative Technical Controls

- Authentication
- Authorization
- Access Control Enforcement
- Nonrepudiation
- Protected Communications
- Transaction Privacy
Detection and Recovery Technical Controls

- Audit
- Intrusion Detection and Containment
- Proof of Wholeness
- Restore Secure State
- Virus Detection and Eradication
Preventative Management Security Controls

- INFOSEC roles and responsibilities including personnel security
- INFOSEC documentation
Detection Management Security Controls

- Implement personnel security controls
- Review controls
- System audits
- Ongoing risk management
- Configuration control
Recovery Management Security Controls

- BCP/DR
- Establish incident response capability
Preventive Operational Security Controls

- Media controls
- Physical environment
- Power control
- Control software viruses
Detective Operational Controls

- Provide physical security
- Environmental security
Residual Risk

Figure 4-4. Implemented Controls and Residual Risk
Evaluation and Assessment

- Systems are dynamic
- Good Security Practices – Periodic risk assessment
- Keys for Success
  1. Senior management’s commitment;
  2. Full IT team support and participation
  3. Risk assessment team competence.
     - Expertise to apply risk assessment methodology to a specific enterprise
     - Ability to identify mission risks
     - Provide cost-effective safeguards meeting needs of the organization
  4. Awareness and cooperation of user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization
  5. An ongoing risk evaluation and assessment process.
Risk Assessment Report

- A management report that helps senior management make decisions on policy, procedural, budget, and system operational and management changes.

- Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

- In the risk assessment report, some people prefer to address the threat/vulnerability pairs as observations instead of findings.
Questions?